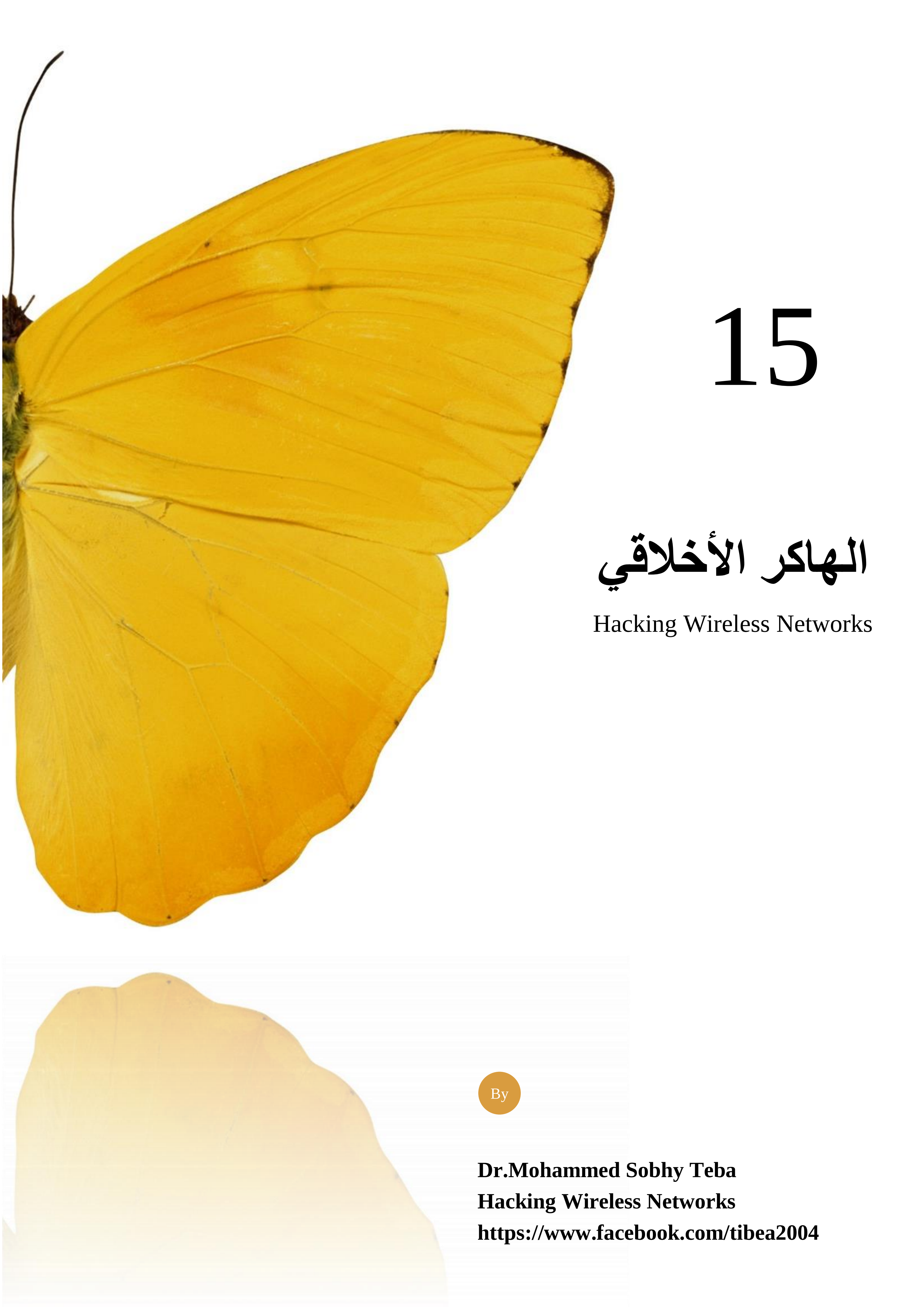


15

الهاكر الأخلاقي

Hacking Wireless Networks

By

Dr.Mohammed Sobhy Teba
Hacking Wireless Networks
https://www.facebook.com/tibea2004

CONTENTS

15.1 مفهوم الشبكات اللاسلكية "WIRELESS CONCEPT"

الشبكات المحلية اللاسلكية (**WLAN**)، أصبح الآن بإمكان الشخص التنقل في اي مكان يريده وحتى بالأماكن العامة وهو حاملا جهازه الحاسب المحمول أو الـ (لاب توب) بدون اي من الأسلاك، يستطيع ان يرسل أو يتلقى اي من البريد الإلكتروني وتصفح الإنترنت بحريه كامله وأصبح بإمكان المسافرين في الأول من أبريل 2004 على متن طائرات لشركة طيران ألمانية خلال الرحلات عبرت المحيط الأطلسي استخدام المحمول للاتصال بالإنترنت وكل هذا بفضل التقنية الجديدة وهي الشبكات المحلية اللاسلكية (**WLAN\wireless local area network**) وتسمح هذه التقنية بالاتصال بشبكة الإنترنت عبر إشارة الراديو (**radio frequency/RF**) بدلا من الاتصال عبر الأسلاك.

لفهم مفهوم قرصنة الشبكات اللاسلكية، دعونا نبدأ مع المفاهيم اللاسلكية.

يقدم هذا القسم نظرة ثاقبة عن الشبكات اللاسلكية، وأنواع الشبكات اللاسلكية والمعايير اللاسلكية، أوضاع وعمليات المصادقة والمصطلحات، وأنواع الهوائي اللاسلكي.

الشبكات اللاسلكية "Wireless Networks"

يشير مصطلح الشبكة اللاسلكية إلى شبكة كمبيوتر غير متصلة بأي نوع من الكابلات. في الشبكات اللاسلكية، يتم نقل البيانات من خلال موجات الراديو. هذا يحدث عادة في الطبقة المادية "**Physical layer**" لهيكل الشبكة.

تم تطوير **Wi-Fi** الى المعيار **IEEE 802.11**، ويستخدم على نطاق واسع في الاتصالات اللاسلكية. فإنه يوفر الوصول اللاسلكي إلى التطبيقات والبيانات عبر شبكة الراديو. **Wi-Fi** يضع العديد من الطرق لبناء اتصال بين المرسل والمتلقي مثل:

- Direct-sequence Spread Spectrum (DSSS)
- Frequency-hopping Spread Spectrum (FHSS)
- Infrared (IR)
- Orthogonal Frequency-division Multiplexing (OFDM)

إيجابيات وسلبيات استخدام الشبكات اللاسلكية

المميزات:

- المرونة (**wirelessness**): للشبكات اللاسلكية فوائد أكثر من الشبكات السلكية وإحدى هذه الفوائد المرونة إذ تمر موجات الراديو بالحيطان والحاسوب اللاسلكي يمكن أن يكون في أي مكان على نطاق الاكسس بوينت.
- التركيب السريع والسهل ويزيل الأسلاك من خلال الجدران والأسقف.
- من الأسهل توفير اتصال لاسلكي في المناطق حيث انه من الصعب وضع كابل.
- يمكن الوصول إلى الشبكة من أي مكان داخل نطاق نقطة الوصول "نطاق الاكسس بوينت".
- باستخدام الشبكة اللاسلكية، يمكن للعديد من الأعضاء الوصول إلى الإنترنت في وقت واحد دون الحاجة إلى اجهزه اضافيه او العديد من الكابلات.
- الأماكن العامة مثل المطارات والمكتبات والمدارس، أو حتى المقاهي توفر لك اتصال إنترنت ثابت وذلك باستخدام الشبكة المحلية اللاسلكية.

على الرغم من هذه الفوائد، فإن الشبكات اللاسلكية لا تخلو من بعض المشاكل لعل أهمها:

العيوب:

- الأمن هي القضية الكبرى والتي قد لا تلبي التوقعات.
- زيادة عدد أجهزة الكمبيوتر على الشبكة، يؤدى الى بطء او معانة عرض النطاق الترددي.
- تغير معايير **Wi-Fi** يؤدي إلى استبدال البطاقات اللاسلكية و/أو نقطة وصول.
- بعض المعدات الالكترونية يمكن أن تتداخل مع شبكات **Wi-Fi**.
- مشكلات التوافق: فالأجهزة المصنوعة من قبل شركات مختلفة قد لا تتمكن من الاتصال مع بعضها أو قد تحتاج إلى جهد إضافي للتغلب على هذه المشاكل.
- الشبكات اللاسلكية تكون غالباً أبطأ من الشبكات الموصولة مباشرةً باستخدام تقنيات الإيثرنت **Ethernet**.
- مخاوف صحية من الشبكات اللاسلكية: في الآونة الأخيرة، ازدادت المخاوف من مخاطر الشبكات اللاسلكية والحقول الكهرومغناطيسية التي تولّدها على الرغم من عدم وجود أدلة قاطعة تثبت صحة هذه الادعاءات. فعلى سبيل المثال، رفض رئيس جامعة **Lakehead** في كندا إنشاء شبكة لاسلكية ضمن حرم الجامعة بسبب دراسة تقول أن تأثير التعرض للحقول

الكهرومغناطيسية الناتجة عن الشبكات اللاسلكية يؤدى الى الإصابة بسرطانات وأورام ولكن يجب أن يُدرس بشكل أكبر قبل تحديد مدى هذا التأثير.

أنواع الشبكات اللاسلكية

فيما يلي أربعة أنواع من الشبكات اللاسلكية:

Extension to a Wired Network

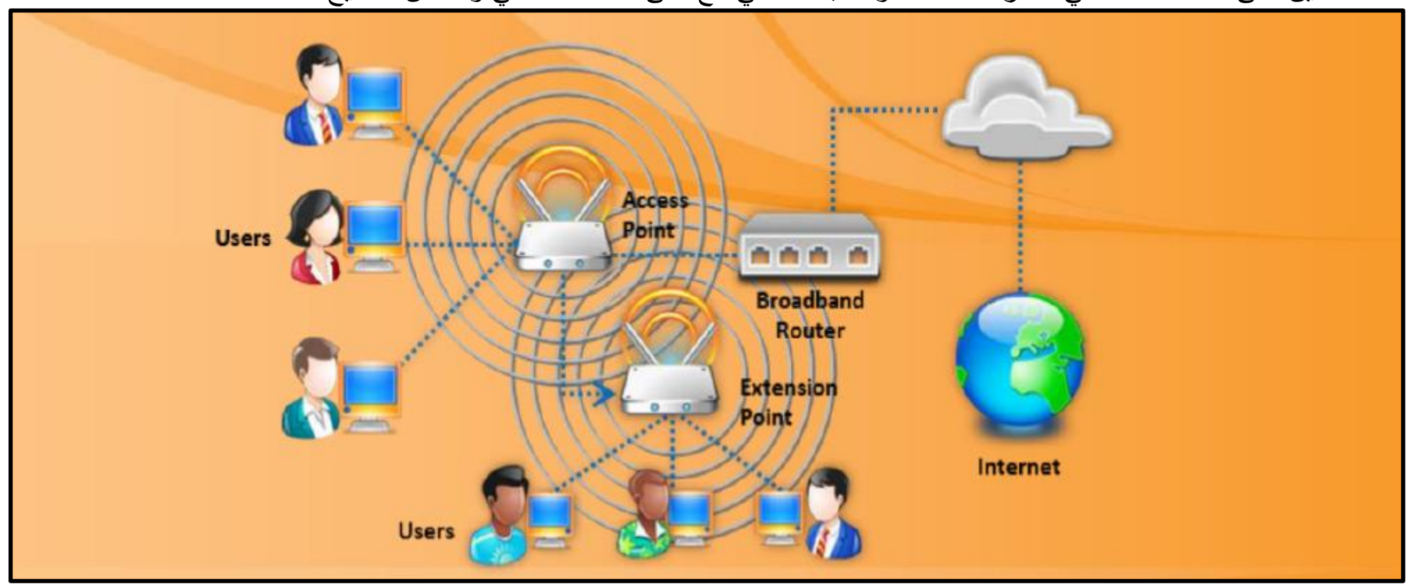
يتكون من الشبكة السلكية والجهاز اللاسلكي "**wireless device**". ونجد هنا ان نقاط الوصول "**access point**" عباره عن نوعين:

- Software access points
- Hardware access points

هنا يمكن إنشاء شبكة لاسلكية باستخدام نقطة الوصول، أو **base station**. مع هذا النوع من الشبكة، نقطة الوصول تتصرف مثل **hub**، وتوفير الاتصال لأجهزة الكمبيوتر اللاسلكية على نظامها. يمكن ربط شبكة محلية لاسلكية إلى **LAN** سلكي، والذي يسمح بوصول الكمبيوتر لاسلكيا إلى موارد **LAN**، مثل خوادم الملفات أو اتصالات الإنترنت الحالية.

Software Access Points (SAPS): يمكن أن يكون متصلا بشبكة سلكية، وتشغيله على جهاز كمبيوتر مجهز ببطاقة شبكة لاسلكية.

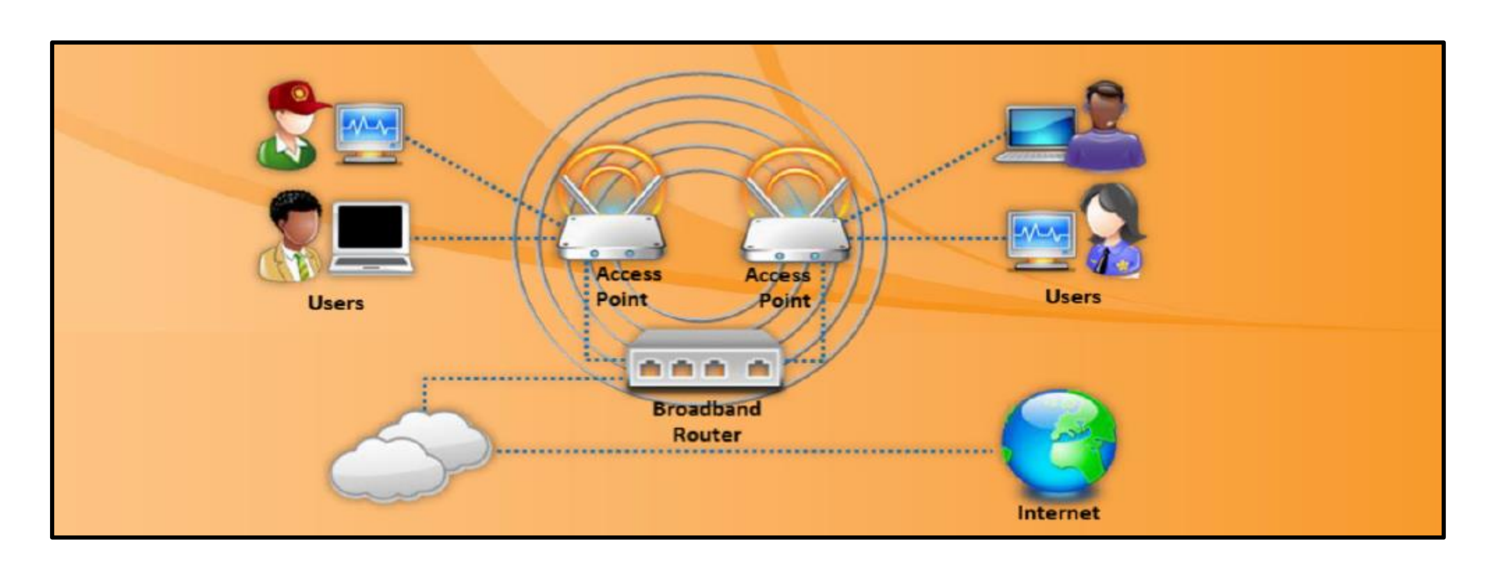
Hardware Access Points (HAPs): يوفر الدعم الشامل لمعظم الخصائص اللاسلكية. مع دعم برامج الشبكات المناسبة، يمكن للمستخدمين على **LAN** اللاسلكي مشاركة الملفات والطابعات التي تقع على **LAN** السلكي والعكس صحيح.



Multiple Access Points

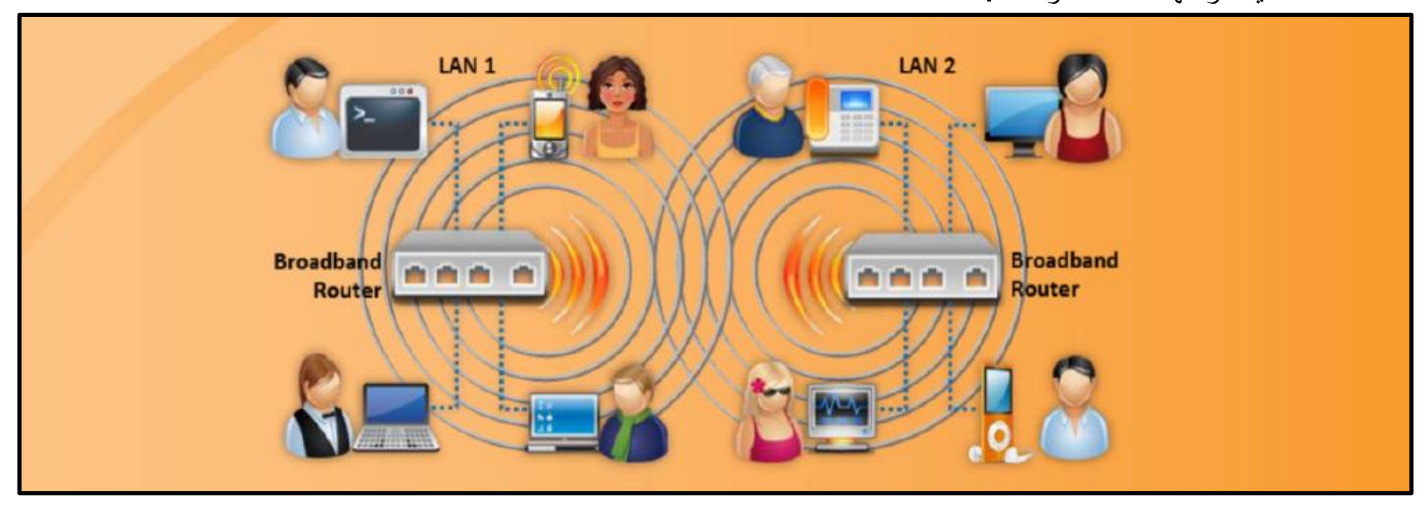
هذا النوع من الشبكة يتكون من أجهزة الكمبيوتر اللاسلكية المتصلة لاسلكيا باستخدام نقاط وصول متعددة. إذا كانت مساحة كبيرة واحدة لا يمكن تغطيتها عن طريق نقطة وصول واحدة، فيمكن إنشاء نقاط وصول متعددة "**multiple access points**" أو **extension points**. لقد تم وضع قدرة **extension points** من قبل بعض المنتجين، ولا يتم تعريفه في المعيار اللاسلكي.

عند استخدام نقاط وصول متعددة، تحتاج كل نقطة وصول لمنطقة لاسلكية التداخل مع منطقة جارتها. وهذا يوفر للمستخدمين القدرة على التحرك السلس باستخدام ميزة تسمى التجوال. بعض الشركات المصنعة تعمل على تطوير **extension points** التي تكون بمثابة التتابع اللاسلكي، وتوسيع نطاق نقطة وصول واحدة. **Extension points** متعددة يمكن ان تعمل معا لتوفير وصول لاسلكي إلى أماكن بعيدة من نقطة الوصول المركزية.



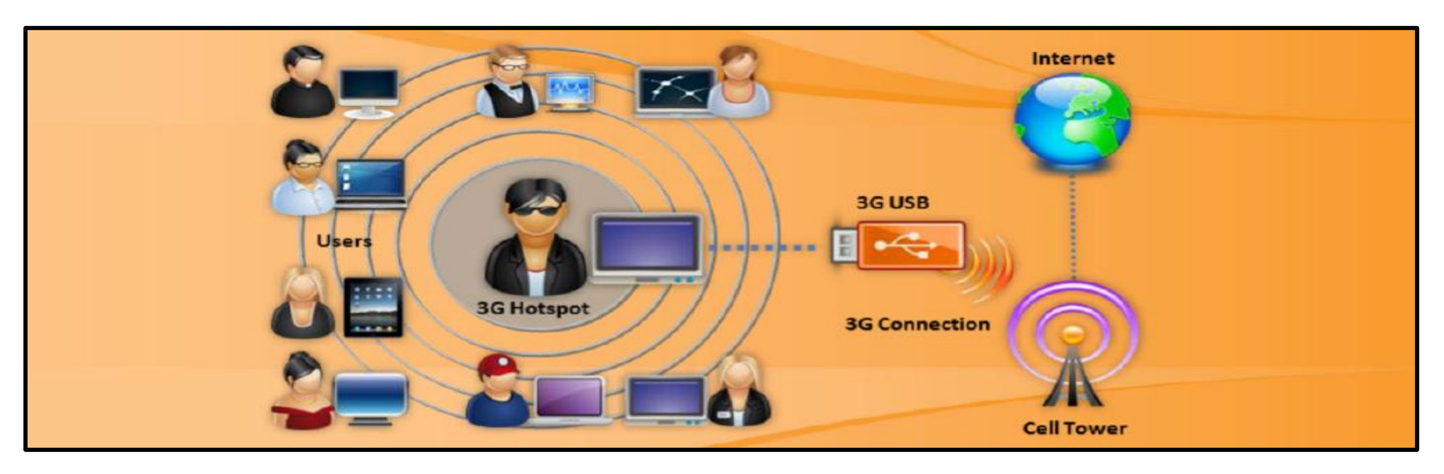
LAN to LAN Wireless Network

توفر نقاط الوصول اتصال لاسلكي لأجهزة الكمبيوتر المحلية، وأجهزة الكمبيوتر المحلية على شبكات مختلفة يمكن أن تكون مترابطة. جميع نقاط الوصول الأجهزة لديها القدرة على أن تكون مترابطة مع نقاط الوصول الأجهزة الأخرى. ومع ذلك، ربط الشبكات المحلية عبر اتصالات لاسلكية هو مهمة ضخمة ومعقدة.



3G Hotspot

هو نوع من الشبكة اللاسلكية التي توفر خدمة **Wi-Fi access** الى أجهزة **Wi-Fi** بما في ذلك مشغلات **MP3**، أجهزة الكمبيوتر المحمولة، الكاميرات، أجهزة **PDAs**، **netbooks**، وأكثر من ذلك.



IEEE 802.11 (WIRELESS STANDARD)

مقدمه:

IEEE هو اختصار لـ **Institute of Electrical and Electronics Engineers** وتعنى جمعية مهندسي الكهرباء والإلكترونيات. هم مجموعة من العلماء والمهندسين والمهنيين الذين يعملون، جنبا إلى جنب، هي السلطة الرائدة في مجال الطيران، والاتصالات، والهندسة الطبية الحيوية، والطاقة الكهربائية. هي منظمة غير ربحية عالمية من أجل تطوير وتعزيز التكنولوجيا المتعلقة بالمعلومات في العالم وتمتلك عدد 400،000 عضو. تم تشكيل **IEEE** في عام 1963 من خلال اندماج:

- جمعية مهندسي الكهرباء الأمريكان "**AIEE**": تأسست عام 1884 تهتم بدراسات أنظمة الطاقة والاضاءة الكهربائية والاتصالات السلكية كالتلغراف أو الهاتف.
- جمعية مهندسي الأمواج الراديوية "**IRE**": تأسست عام 1912 وتتعلق بالراديو بالغالب.

مع تطور الإلكترونيات بشكل هائل منذ مطلع الثلاثينات بدأت رقعة الدراسات والمصطلحات العلمية بالتوسع، مما دفع الجمعيتين إلى توسيع حدود شموليتهما التقنية بشكل تدريجي إلى حد أصبح معه يصعب التمييز بين مجال كل من الجمعيتين وأصبح الوضع تنافسيا خلال فترة الحرب العالمية الثانية، وأخير تم الاتفاق 1961 وتم دمج الجمعيتين بشكل رسمي عام 1963.

تم فصل **IEEE** الى لجان مختلفة. لجنة "**802**" المسؤولة عن تطور معايير:

Local Area Network (LAN) - Metropolitan Area Network (MAN)

وأكثر المعايير المعروفة جيدا هي **Ethernet**، **Token Ring**، **Wireless LAN**، **Bridging**، و**Virtual Bridged LANs**.

مواصفات **IEEE** تشمل أدنى اثنين من طبقات **OSI** التي تحتوي على الطبقات **physical** و**link**. تنقسم طبقة **link** الى اثنين من الطبقات الفرعية تسمى **Logical Link Control (LLC)** و **Media Access Control (MAC)**.

يسرد الجدول التالى من ويكيبيديا لجان IEEE المختلفة:

Name	Description	Note
IEEE 802.1	Bridging (networking) and Network Management	
IEEE 802.2	LLC	inactive
IEEE 802.3	Ethernet	
IEEE 802.4	Token bus	disbanded
IEEE 802.5	Defines the MAC layer for a Token Ring	inactive
IEEE 802.6	MANs (DQDB)	disbanded
IEEE 802.7	Broadband LAN using Coaxial Cable	disbanded
IEEE 802.8	Fiber Optic TAG	disbanded
IEEE 802.9	Integrated Services LAN (ISLAN or isoEthernet)	disbanded
IEEE 802.10	Interoperable LAN Security	disbanded
IEEE 802.11	Wireless LAN (WLAN) & Mesh (Wi-Fi certification)	
IEEE 802.12	100BaseVG	disbanded
IEEE 802.13	Unused[2]	Reserved for Fast Ethernet development[3]
IEEE 802.14	Cable modems	disbanded
IEEE 802.15	Wireless PAN	
IEEE 802.15.1	Bluetooth certification	
IEEE 802.15.2	IEEE 802.15 and IEEE 802.11 coexistence	
IEEE 802.15.3	High-Rate wireless PAN (e.g., UWB, etc.)	
IEEE 802.15.4	Low-Rate wireless PAN (e.g., ZigBee, WirelessHART, MiWi, etc.)	
IEEE 802.15.5	Mesh networking for WPAN	
IEEE 802.15.6	Body area network	
IEEE 802.16	Broadband Wireless Access (WiMAX certification)	
IEEE 802.16.1	Local Multipoint Distribution Service	
IEEE 802.17	Resilient packet ring	
IEEE 802.18	Radio Regulatory TAG	
IEEE 802.19	Coexistence TAG	
IEEE 802.20	Mobile Broadband Wireless Access	
IEEE 802.21	Media Independent Handoff	
IEEE 802.22	Wireless Regional Area Network	
IEEE 802.23	Emergency Services Working Group	
IEEE 802.24	Smart Grid TAG	New (November, 2012)
IEEE 802.25	Omni-Range Area Network	Not yet ratified

IEEE 802.11

هو اسم لسلسلة من البروتوكولات للشبكات اللاسلكية قام بها مجموعة العمل 11 من **IEEE**. تسمى أحياناً "**WLAN**" أو "**WiFi**". لمزيد من المعلومات يمكنك زيارة رابط ويكيبيديا التالي:

http://en.wikipedia.org/wiki/IEEE_802.11

معايير وتعديلات 802.11 "Standards and Amendments 802.11"

الجدول التالي، مع بيانات من ويكيبيديا، يسرد معايير جمعية **IEEE** والتعديلات لفريق العمل **IEEE 802.11**.

IEEE 802.11-1997: The WLAN standard was originally 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and infrared (IR) standard (1997), all the others listed below are Amendments to this standard, except for Recommended Practices 802.11F and 802.11T.

IEEE 802.11a: 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)

IEEE 802.11b: Enhancements to 802.11 to support 5.5 Mbit/s and 11 Mbit/s (1999)

IEEE 802.11c: Bridge operation procedures; included in the IEEE 802.1D standard (2001)

IEEE 802.11d: International (country-to-country) roaming extensions (2001)

IEEE 802.11e: Enhancements: QoS, including packet bursting (2005)

IEEE 802.11F: Inter-Access Point Protocol (2003) Withdrawn February 2006

IEEE 802.11g: 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)

IEEE 802.11h: Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)

IEEE 802.11i: Enhanced security (2004)

IEEE 802.11j: Extensions for Japan (2004)

IEEE 802.11-2007: A new release of the standard that includes amendments a, b, d, e, g, h, i, and j. (July 2007)

IEEE 802.11k: Radio resource measurement enhancements (2008)

IEEE 802.11n: Higher-throughput improvements using MIMO (multiple-input, multiple-output antennas) (September 2009)

IEEE 802.11p: WAVE—Wireless Access for the Vehicular Environment (such as ambulances and passenger cars) (July 2010)

IEEE 802.11r: Fast BSS transition (FT) (2008)

IEEE 802.11s: Mesh Networking, Extended Service Set (ESS) (July 2011)

IEEE 802.11T: Wireless Performance Prediction (WPP)—test methods and metrics Recommendation cancelled

IEEE 802.11u: Improvements related to HotSpots and 3rd-party authorization of clients, e.g., cellular network offload (February 2011)

IEEE 802.11v: Wireless network management (February 2011)

IEEE 802.11w: Protected Management Frames (September 2009)

IEEE 802.11y: 3650–3700 MHz Operation in the U.S. (2008)

IEEE 802.11z: Extensions to Direct Link Setup (DLS) (September 2010)

IEEE 802.11-2012: A new release of the standard that includes amendments k, n, p, r, s, u, v, w, y, and z (March 2012)

IEEE 802.11aa: Robust streaming of Audio Video Transport Streams (June 2012)

IEEE 802.11ac: Very High Throughput <6 GHz;[44] potential improvements over 802.11n: better modulation scheme (expected ~10% throughput increase), wider channels (estimate in future time 80 to 160 MHz), multi user MIMO;[45] (December 2013)

IEEE 802.11ad: Very High Throughput 60 GHz (December 2012) – see WiGig
IEEE 802.11ae: Prioritization of Management Frames (March 2012)
IEEE 802.11af: TV Whitespace (February 2014)

معايير مازالت في مرحلة التطوير

IEEE 802.11mc: Roll-up of 802.11-2012 with the aa, ac, ad, ae & af amendments to be published as 802.11-2016 (~ March 2016)
IEEE 802.11ah: Sub 1 GHz license exempt operation (e.g., sensor network, smart metering) (~ March 2016)
IEEE 802.11ai: Fast Initial Link Setup (~ November 2015)
IEEE 802.11aj: China Millimeter Wave (~ June 2016)
IEEE 802.11ak: General Links (~ May 2016)
IEEE 802.11aq: Pre-association Discovery (~ July 2016)
IEEE 802.11ax: High Efficiency WLAN (~ May 2018)
IEEE 802.11ay: Enhancements for Ultra High Throughput in and around the 60 GHz Band (~ TBD)
IEEE 802.11az: Next Generation Positioning (~ TBD)

802.11F and 802.11T are recommended practices rather than standards, and are capitalized as such. 802.11m is used for standard maintenance. 802.11ma was completed for 802.11-2007, 802.11mb was completed for 802.11-2012, and 802.11mc is working towards publishing 802.11-2016.

يقدم الجدول أعلاه مجرد لمحة عامة عن المعايير والتعديلات المختلفة. وبطبيعة الحال، لا حاجة لحفظ كل منهم ولكن من المهم أن نتذكر ما يلي:

802.11 – The original WLAN standard
802.11a – Up to 54 Mbit/s on 5 GHz
802.11b – 5.5 Mbit/s and 11 Mbit/s on 2.4 GHz
802.11g – Up to 54 Mbit/s on 2.4 GHz. Backward compatible with 802.11b
802.11i – Provides enhanced security
802.11n – Provides higher throughput with Multiple Input/Multiple Output (MIMO)

البروتوكولات الأساسية لمعيار 802.11 "Main 802.11 Protocols"

يسرد الجدول التالي أهم بروتوكولات 802.11 بجانب بعض من خصائصهم:

Protocol	Release Date	Frequencies	Rates	Modulation	Channel Width	Notes
Legacy	1997	2.4-2.5GHz	1 or 2Mbit	FHSS/DSSS	1MHz/20MHz	No implementations were made for IR
802.11b	1999	2.4-2.5GHz	1, 2, 5.5, 11Mbit	DSSS	22MHz	Proprietary extension: up to 33Mbit
802.11a	1999	5.15-5.25/5.25-5.35/5.725-5.875GHz	6, 9, 12, 18, 24, 36, 48, 54Mbit	OFDM	20MHz	Proprietary extension: up to 108MBit
802.11g	2003	2.4-2.5GHz	Same as 802.11a and 802.11b	DSSS /OFDM	20MHz/22MHz	Proprietary extensions: up to 180Mbit/125MBit
802.11n	2009	2.4 and/or 5GHz	Up to 600Mbit	DSSS/OFDM	20/20 or 40MHz	

ملاحظة: ملحقات الامتداد "**Proprietary extensions**" كما قلنا سابقا ليست موحدة وسوف تعمل فقط عندما يكون العميل والاكسيس بوينت لديهم نفس التقنيات، مما يؤدى إلى ارتفاع جودة الإشارة.

وصف البروتوكولات

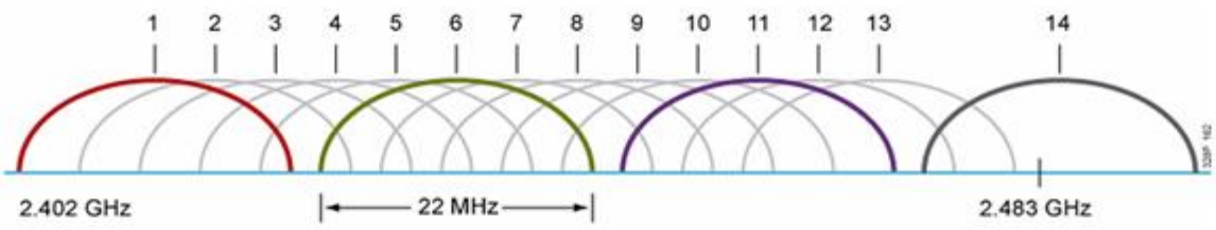
- **IEEE 802.11**

هو المعيار الأصلي أو الأساسي للشبكات اللاسلكية، والذي ظهر في بداية الأمر حيث تم إطلاقه عام 1997، ويعمل بمعدل نقل بيانات 1 الي 2 ميجابت لكل ثانية وعلى التردد 2.4 جيجا، ويمكن استخدامه مع الأشعة تحت الحمراء "**infrared**"، او من خلال ترددات الراديو في **Direct-Sequence Spread-Spectrum (DSSS)** و**Frequency Hopping Spread-Spectrum (FHSS)**.
IEEE 802.11 يعرف أيضا بـ **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)** ، كطريقة **medium access**. في **CSMA**، المحطة تنوي إرسال البيانات على وسائط لديها للاستماع لفترة محددة سلفا من الوقت لضمان عدم وجود نظام آخر يرسل في الوقت نفسه. في **CSMA/CA**، النظام الذي يعتزم بإرسال البيانات يقوم أولا بإرسال إشارة على الشبكة لإخبار جميع المحطات الأخرى ان لا تقوم بالإرسال، ثم يقوم هو فقط بإرسال البيانات الخاصة به. بالإضافة إلى **CSMA/CA**، يمكن استخدام **Request to Send/Clear to Send (RTS/CTS)** أيضا لتجنب الاصطدامات. يبدو أن التطور المعلوماتي واللاسلكي جعل المعيار الأصلي غير كاف لتلبية متطلبات الزيادة في السرعة فمنذ 1999 تم البدء في إطلاق العديد من المعايير التي تتباين فيها السرعة والتردد وكذلك الخدمات الإضافية من الأمن وكمقدمة لما سوف نستفيض في بعضه فهذا مختصر لتلك المعايير التي تم اطلاقها واعتمد عليه في عالم الشبكات اللاسلكية.

- **IEEE 802.11b**

هو تعديل للمعيار الأصلي **802.11** يعمل على التردد 2.4 جيجا هرتز (**2.4GHz - 2.485GHz**) وهذا يسمح بوجود 14 قناة ترددية بحد أقصي وذلك تبعا للبلد التي ستعمل فيها شبكتك اللاسلكية. قام بإضافة التعديل **Complementary Code Keying (CCK) coding** الى المعيار الأصلي لكي يعمل بسرعتي 5.5 و11 ميجابت لكل ثانية وتم اطلاقه في 1999.
هذه القنوات 14 الترددية لديها عرض من **22MHz** حول التردد مركزي. يبين الجدول التالي العلاقة بين رقم كل قناة والتردد المقابلة لها:

Channel	Central Frequency
1	2.412 GHz
2	2.417 GHz
3	2.422 GHz
4	2.427 GHz
5	2.432 GHz
6	2.437 GHz
7	2.442 GHz
8	2.447 GHz
9	2.452 GHz
10	2.457 GHz
11	2.462 GHz
12	2.467 GHz
13	2.472 GHz
14	2.477 GHz



بحساب سريع يظهر أنه من الممكن أن يكون هناك فقط 3 قنوات غير متداخلة ويميل توافر القناة وفقا للمعايير المحلية لكل بلد أو منطقة. مثلا:

- USA – Uses channels 1 to 11 (2.412 GHz – 2.462 GHz)

- Europe – Uses channels 1 to 13 (2.412 GHz – 2.472 GHz)
- Japan – Uses channels 1 to 14 (2.412 GHz – 2.484 GHz)

- **IEEE 802.11a**

تم إطلاق هذا المعيار في نفس الوقت تقريبا من إطلاق المعيار **802.11b** ولكن نظرا لعدم وجود، وارتفاع أسعار، أجهزته، فإنه لم يكن لديه الكثير من النجاح. يعمل على التردد 5 جيجا هرتز والذي يحمل اثنين من الميزات عن 2.4 جيجا هرتز الذي يستخدم من قبل المعيار **802.11b**:

- التردد 2.4 جيجا هرتز مزدحم للغاية مع الأجهزة الأخرى مثل الهواتف اللاسلكية، وأجهزة البلوتوث، وحتى أفران الميكروويف.
- التردد 5 جيجا هرتز لديها أكثر بكثير من القنوات المتاحة وأنها لا تتداخل مثل تلك الموجودة في التردد 2.4 جيجا هرتز.

في المعيار **802.11a** يستخدم **Orthogonal Frequency-Division Multiplexing (OFDM)** لتعديل الإشارة ويوفر سرعة نقل بيانات 54 ميجا بت لكل ثانية. الترددات المسموح بها يمكن ان تختلف تبعا للموقع الخاص بك ولكن بشكل عام تتراوح من 5.15 – 5.35 جيجا هرتز وهو للاستخدام في الأماكن المغلقة و5.8 – 5.7 جيجا هرتز وهي مخصصة للاستخدام في الهواء الطلق.

- **IEEE 802.11g**

يستخدم معيار **802.11g** نفس معدل الإشارة المعتمدة في معيار **802.11a** ولكن على تردد 2.4 جيجا هرتز، مما أدى إلى نفس معدلات السرعة. نطاق الإشارة هو أفضل قليلا من **802.11a** وهو متوافق مع المعيار **802.11b**. تم اطلاقه في 2003.

- **IEEE 802.11n**

بدأ العمل بهذا المعيار في عام 2004 مع تحسين معدلات النقل وتوفير المزيد من النطاق في شبكات 2.4 جيجا هرتز و5 جيجا هرتز. بعد اثنين من سنوات العمل، تم الإفراج عن النسخة الأولى مما سمح بسرعة تصل إلى 74 ميجا بت لكل ثانية. ثم في عام 2007 تم الافراج عن النسخة الثانية والتي تسمح العمل بسرعة تصل إلى 300 ميجا بت لكل ثانية. وأخيرا، في عام 2009، تم الانتهاء من الإصدار الأخير من معيار **802.11n**.

الزيادة في هذه السرعة في المعيار **802.11n** ناتج عن استخدام تقنية الاتصال **Multiple-Input Multiple-Output (MIMO)**.

باختصار، **MIMO** يستخدم هوائيات متعددة، كل مع جهاز إرسال واستقبال خاص به ويستغل ظاهرة موجات الراديو المتعددة، حيث ترتد الإشارة على كافة الكائنات مثل الجدران والأبواب، وما إلى ذلك. هذا المعيار يسمح لاستخدام ما يصل إلى 4 هوائيات مما ينتج عن المزيد من التيارات التي يجري إرسالها واستقبالها وبالتالي، معدل نقل أفضل بكثير. عرض القناة يمكن أن يكون 40 ميغا هرتز بدلا من 20 ميغا هرتز، وبالتالي مضاعفة سرعة نقل البيانات.

هناك أيضا طريقة جديدة تسمى **Greenfield mode** والتي تقدم ديباجة جديدة لمعيار **802.11n** حيث الأجهزة الوحيدة العاملة في معيار **802.11n** فقط سوف يسمح لها على الشبكة.

- **IEEE 802.11i**

في 2007 تم إطلاق هذا المعيار لتوصيف طرق تأمين أكثر قسوة من الطرق السابقة **WAP** وذلك مع البروتوكول **WPA** وتحسيناته **WPA 2**.

- **IEEE 802.16a/d//e/m (WiMAX)**

نظام الواي ماكس **WiMAX**. هذه الكلمة هي اختصارا للمصطلح **Worldwide Interoperability for Microwave Access** ويعرف أيضا باسم **802.16**. الواي ماكس **WiMAX** نظام جديد للاتصال السريع بالأنترنت وسوف يستبدل نظام الكابل ونظام الـ **DSL** للاتصال بشبكة الانترنت من أي مكان وبدون أسلاك. تشبه فكرة عمل الواي ماكس فكرة عمل **WiFi** ولكن تقنية الواي ماكس تعمل على مسافات أكبر وبسرعات أعلى وتوفر خدمة الانترنت لعدد كبير من المستخدمين. هذا بالإضافة إلى ان الواي ماكس سوف تصل لكل الناس حتى لو لم تكن لديهم خدمات الهاتف أو خدمة الاتصال بالأنترنت بواسطة الكوابل.

أسرع وسيلة اتصال **WiFi** تستطيع ان ترسل بيانات بسرعة **54 Mbps** في أفضل الظروف ولكن الواي ماكس تستطيع ان ترسل البيانات بسرعة **70-1000 Mbps**. هذا بالإضافة إلى ان **WiFi** تعمل على مسافات في حدود 30 متر فان الواي ماكس تعمل على مسافات تصل إلى 50 كيلومتر. وهذا يعود إلى الترددات المستخدمة في تقنية الواي ماكس وكذلك قدرة محطات الإرسال.

يستند الواي ماكس (**IEEE 802.16**) تحديدا في الطبقة المادية العاملة في نطاق 10-66 جيجا هرتز. 802.16a، قد استكملت في عام 2004 ليصبح **802.16a-2004** حيث أضاف النطاق 2 إلى 11 جيجا هرتز. تم تحديثه الى المعيار **802.16e-2005** في عام 2005، ويستخدم (**(OFDM) Orthogonal frequency-division multiplexing**) وهي طريقة لترميز البيانات الرقمية على الترددات الحاملة المتعددة.

- **Bluetooth**

هو بروتوكول لاسلكي يقصد في الغالب ليتم استخدامه من قبل العروض قصيرة المدى.

Service Set Identifier (SSID)

The Service Set Identifier (SSID) هو معرف فريد يتم استخدامه لإنشاء والحفاظ على الاتصال اللاسلكي. **SSID** هو **token** لتحديد شبكة (**الواي فاي**) "**شبكة 802.11**". افتراضيا هو جزء من رأس الحزمة "**Packet header**" التي يتم ارسالها عبر الشبكة اللاسلكية (**WLAN**). هي بمثابة كلمة السر الواحدة المشتركة بين نقاط الوصول والعملاء. المخاوف الأمنية تنشأ عندما لا يتم تغيير القيم الافتراضية، حيث ان هذه الوحدات تصبح عرضه للاختراق بسهولة. نقاط الوصول **SSID** تبث إشارات الراديو باستمرار التي يتم استقبالها من قبل أجهزة المضيفين عند تمكينه. وضع الوصول الغير آمن تتواصل مع نقاط الوصول من خلال بث **configured SSID**، **blank SSID**، أو **SSID** تم اعداده بأنه "**any**". ولأن **SSID** هو اسم فريد يعطى الى **WLAN**، فيجب على جميع الأجهزة ونقاط الوصول الموجودة في **WLAN** استخدام نفس **SSID**. ومن الضروري لأي جهاز يريد الانضمام إلى **WLAN** إعطاء نفس **SSID** الفريد من نوعه. إذا تم تغيير **SSID** للشبكة، فمن الضروري إعادة إعداد **SSID** في كل شبكة، باعتبار أن كل مستخدم في الشبكة يقوم بإعداد **SSID** في النظام الخاص به. للأسف، **SSID** لا يوفر الأمن الى **WLAN**، حيث انه يمكن التنصت عليه في صورة نص عادي "**plain text**" من الحزم. يشار أيضا إلى **SSID** بانه اسم الشبكة لأن الأساس هو الاسم الذي يعرف الشبكة اللاسلكية.

SSID يمكن أن يصل إلى 32 حرفا. حتى لو كانت نقاط الوصول (**APs**) من هذه الشبكات هي قريبة جدا، وحزم الاثنين لن يتداخلا. وهكذا، يمكن اعتبار **SSID** بانه كلمة المرور الى **AP**، ولكن يمكن إرسالها في نص واضح ويمكن اكتشافه بسهولة. وبعبارة أخرى، **SSID** يمكن أن يسمى بالسر المشترك الذي يعلمه الجميع، ويمكن لأي شخص أن يحدده. يبقى **SSID** سري فقط على الشبكات المغلقة مع أي نشاط، وهو غير مريح للمستخدمين الشرعيين. **SSID** هو المفتاح السري بدلا من المفتاح العمومي. بعض **SSID** الاكثر شيوعا هي:

- **comcomcom**
- **Default SSID**
- **Intel**
- **Linksys**
- **Wireless**
- **WLAN**

WI-FI AUTHENTICATION MODES

مصادقة الواي فاي يمكن أن تؤدي في وضعين:

- **نظام التوثيق المفتوح "Open system authentication".**
- **مصادقة المفاتيح المشتركة "Shared key authentication".**

Open System Authentication Process

في عملية المصادقة في نظام التوثيق المفتوح، يمكن لأي محطة لاسلكية ان تقوم بإرسال طلب المصادقة. في هذه العملية، يمكن للمحطة الواحدة إرسال إطار إدارة المصادقة يحتوي على هوية محطة الإرسال، وذلك للحصول على المصادقة والاتصال مع غيرها من المحطات اللاسلكية. المحطة اللاسلكية الأخرى (**AP**) تتحقق من **SSID** العميل التي ورد ومن ثم ترسل إطار التحقق من التوثيق، وهذا إذا تطابق **SSID** في الاصل. بمجرد أن يصل إطار التحقق الى العميل، فان العميل يقوم بالاتصال بالشبكة أو المحطة اللاسلكية.

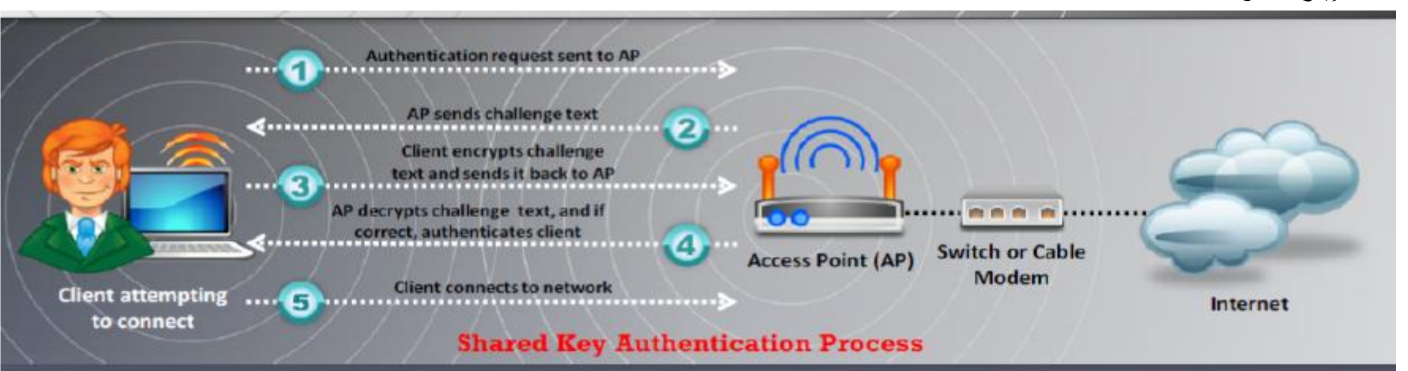


Shared Key Authentication Process

في هذه العملية يفترض ان كل محطة لاسلكية قد تتلقى مفتاح سري مشترك عبر قناة آمنة والتي تختلف عن قنوات الاتصال بالشبكة اللاسلكية **802.11**. توضح الخطوات التالية كيف يتم تأسيس الاتصال في عملية مصادقة المفاتيح المشتركة:

- المحطة ترسل طلب المصادقة إلى نقطة الوصول.
- نقطة الوصول ترسل **challenge text** الى المحطة.
- المحطة قوم بتشفير **challenge text** من خلال استخدام التكوين 64 بت أو 128 بت للمفتاح الافتراضي الخاصة به، ويرسل النص المشفر إلى نقطة وصول.
- تستخدم نقطة الوصول مفتاح **WEP** المكون الخاص بها (الذي يتوافق مع المفتاح الافتراضي للمحطة) لفك تشفير النص المشفر. نقطة الوصول تقارن النص المفكوك مع النص **challenge text** الأصلي. فإذا تمت المطابقة، فان نقطة الوصول تصادق المحطة.
- المحطة تربط بالشبكة.

يمكن لنقطة الوصول رفض مصادقة محطة إذا كان النص المشفر لا يتطابق مع النص الأصلي، ثم لن تكون قادرة على التواصل مع أي شبكة إيثرنت أو شبكات **802.11**.

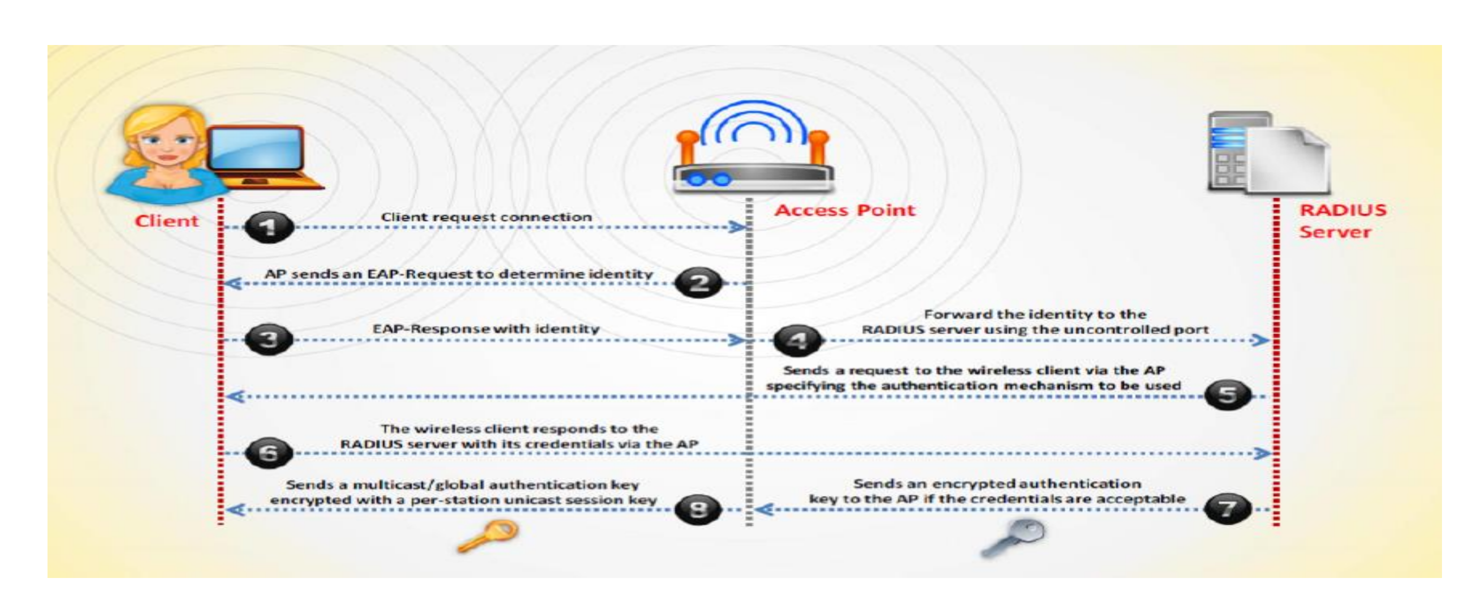


Wi-Fi Authentication Process Using a Centralized Authentication Server

يوفر **802.1x** المصادقة المركزية "**centralized authentication**". لكي تعمل مصادقة **802.1x** على الشبكة اللاسلكية، فيجب على نقطة الوصول "**AP**" أن يكون قادرا على تحديد آمن حركة المرور من العميل اللاسلكي. يتم إنجاز التحديد باستخدام مفاتيح المصادقة التي يتم إرسالها إلى **AP** والعميل اللاسلكي من الخادم **Remote Authentication Dial in User Service (RADIUS)**.

عندما يأتي العميل اللاسلكي ضمن نطاق نقطة الوصول AP، تحدث العملية التالية:

- يرسل العميل طلب المصادقة إلى **AP** لإجراء الاتصال.
- **AP** يرسل **EAP-Request** لتحديد العميل.
- يستجيب العميل اللاسلكي مع الهوية **EAP-Response**.
- **AP** تعمل على توجيه الهوية إلى خادم **RADIUS** باستخدام منفذ **uncontrolled**.
- الخادم **RADIUS** يرسل طلب إلى المحطة اللاسلكية عبر **AP**، مع تحديد آلية المصادقة لاستخدامها.
- المحطة اللاسلكية تستجيب إلى خادم **RADIUS** مع أوراق اعتمادها "**credentials**" عبر **AP**.
- إذا كانت أوراق الاعتماد مقبولة، خادم **RADIUS** يرسل مفتاح المصادقة المشفر إلى **AP**.
- **AP** يولد مفتاح المصادقة العالمي المشفر مع مفتاح جلسة الإرسال "**per-station unicast session key**"، ويحيله إلى المحطة اللاسلكية.

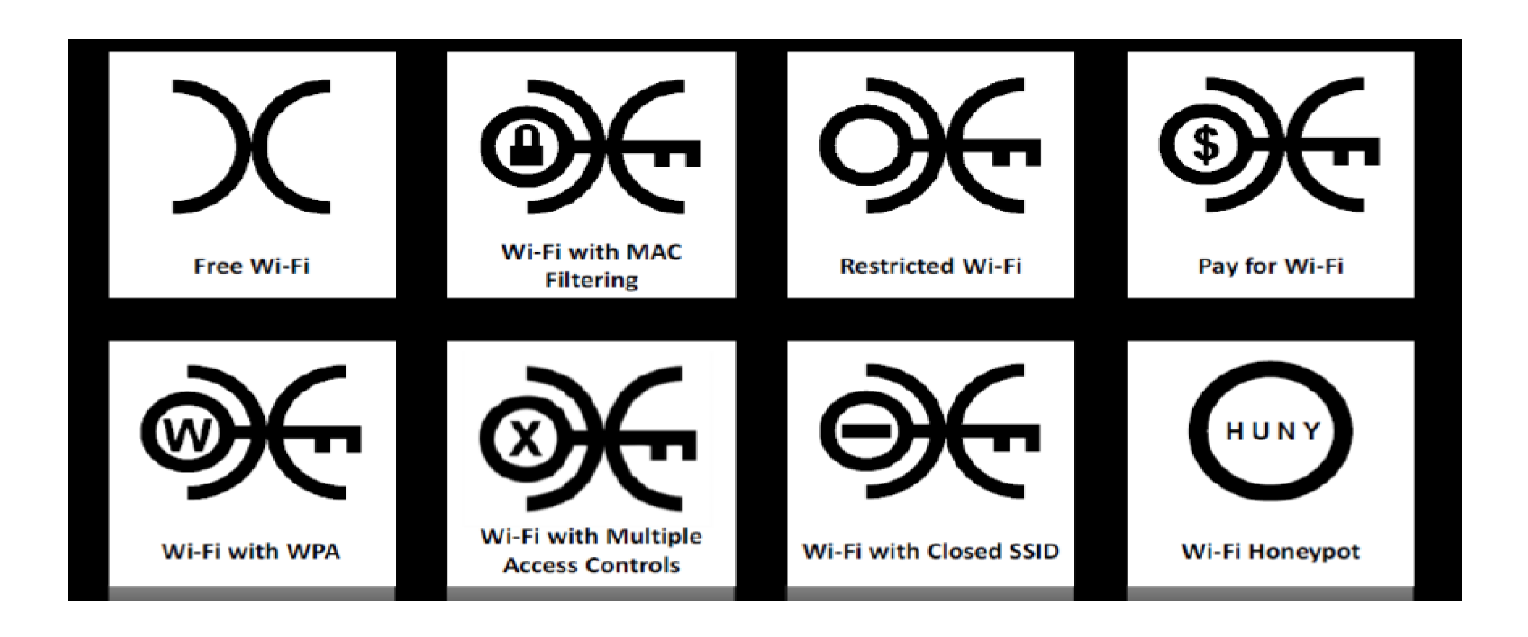


مصطلحات الشبكات اللاسلكية "WIRELESS TERMINOLOGIES"

- **GSM**: كلمة **GSM** هي اختصار لـ **Global System for Mobile Communication** و إذا اردنا ان نترجمها حرفيا الى العربي فهي تعني النظام العالمي للاتصال المتحرك (**الجوال**)، و هي الشبكة الحالية المتوافقة المواصفات في جميع بلدان العالم ويستخدم في اتصال الأجهزة الخليوية مع بعضها البعض.
- **Association:** هي عملية ربط الجهاز اللاسلكي إلى نقطة الوصول "**AP**".
- **BSSID**: هو عنوان **MAC** لنقطة الوصول التي أنشأت مجموعة الخدمات الأساسية.
- **Hotspot:** هو المكان الذي يوجد ويكون فيه الشبكة اللاسلكية متاحة للاستخدام العام.
- **Access Point:** يستخدم لربط الأجهزة اللاسلكية بشبكة الواي فاي.
- **ISM band**: هو نطاق ترددات الراديو الذى تم تعيينه للاستخدام من قبل المستخدمين الغير مرخص لهم و يستخدم هذا النطاق في الأجهزة الطبية و المنزلية و الصناعية التي تتعامل مع ترددات عالية مثل أجهزة الميكروويف المنزلية و بعض أجهزة الأشعة الطبية و الصناعية.
- **Bandwidth:** يصف كمية المعلومات التي يمكن بثها عبر الاتصال.
- **DSSS**: هو اختصار لـ **Direct Sequence Spread Spectrum** يستخدم هذا لنقل البيانات ضمن مجموعة ثابتة من نطاق التردد.
- **FHSS:** هو اختصار لـ **Frequency Hopping Spread Spectrum** ويستخدم لنقل البيانات باستخدام القفز الترددي فإن التردد المخصص لمستخدم معين يتغير باستمرار وبذلك يتنقل المستخدم خلال المكالمة الواحدة إلى قنوات مختلفة يصل عددها إلى 124 قناة. ويتم الانتقال من قناة إلى قناة أخرى بمعدل معين وفي فترات زمنية محددة متفق عليها ويجب أن يتم ذلك بالتنسيق الدائم بين المرسل والمستقبل ويكون الفرق بين التردد المخصص لوصلة الهبوط والتردد المخصص لوصلة الصعود ثابت دائماً وهو **45 MHz**.
- **OFDM:** هو طريقة ترميز البيانات الرقمية على الترددات الحاملة المتعددة مع overlapping radio frequency carriers المتعددة.

WARCHALKING

هو رسم الرموز في الأماكن العامة للإعلان عن شبكة واي فاي المفتوحة. مستوحاة من رموز **hobo**، وتصور علامات **warchalking** من قبل مجموعة من الأصدقاء في يونيو 2002 ونشرت من قبل مات جونز الذي صمم مجموعة من الرموز وأنتج وثيقة قابلة للتحميل تحتوي عليها.

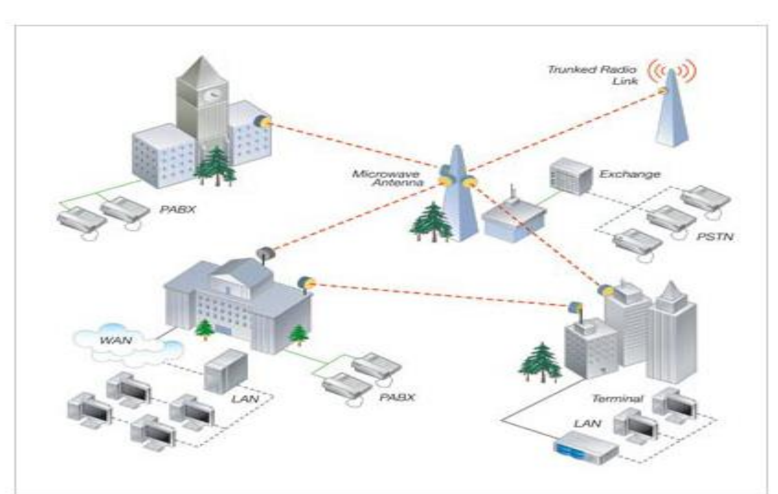


أنواع هوائيات الشبكات اللاسلكية "TYPES OF WIRELESS ANTENNAS"

الهوائيات مهمة لإرسال واستقبال إشارات الراديو. ويمكنهم تحويل النبضات الكهربائية إلى إشارات الراديو والعكس بالعكس. أساسا هناك خمسة أنواع من الهوائيات اللاسلكية:

- النوع الاول: Directional Antennas

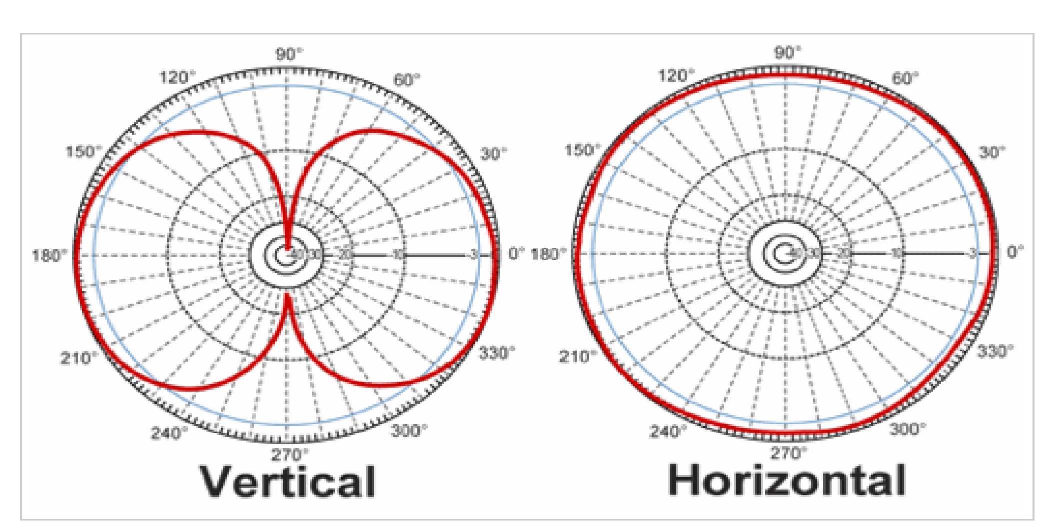
إن هوائيات البث المباشر (**Directional Antennas**) تستخدم للبث بشكل مباشر ومركز من نقطة إلى نقطة. على سبيل المثال (شركتان تبعدان عن بعضهما 10 كيلو مربوطتان بشبكة لاسلكية) أو في بعض الأحيان من نقطة إلى عدة نقاط مثل (فروع الجامعة مرتبطة بفرع واحد لاسلكياً). ومن هنا يتضح أننا نستخدم هذا النوع من الهوائيات لربط الشبكات المتباعدة عن بعضها لاسلكياً كما هو موضح بالصورة التالية:



يستخدم هوائيات البث المباشر للبث والحصول على موجات الراديو من اتجاه واحد. من أجل تحسين الإرسال والاستقبال تم تصميم الهوائيات على العمل بفعالية في عدد قليل من الاتجاهات بالمقارنة مع اتجاهات أخرى. وهذا يساعد أيضا في الحد من التدخل.

- النوع الثاني: Omni-directional

هذا النوع من الهوائيات هو من أكثر الأنواع شيوعاً وذلك لقدرته على البث بشكل حلقي أي 360 درجة وذلك بتوزيع طاقته على كل الاتجاهات بشكل متساوي. وفي هذه الحالة يكون البث بالاتجاه الأفقي (**Horizontal**). وأيضاً يمكن تركيز طاقة هذا الهوائي في اتجاهين متعاكسين وذلك عندما يكون البث بالاتجاه العمودي (**Vertical**) حيث يمكنك التلاعب بالإعداد من خلال الـ **Access Point** المركب عليه الهوائي. والمخطط التالي يظهر البث في الحالتين:



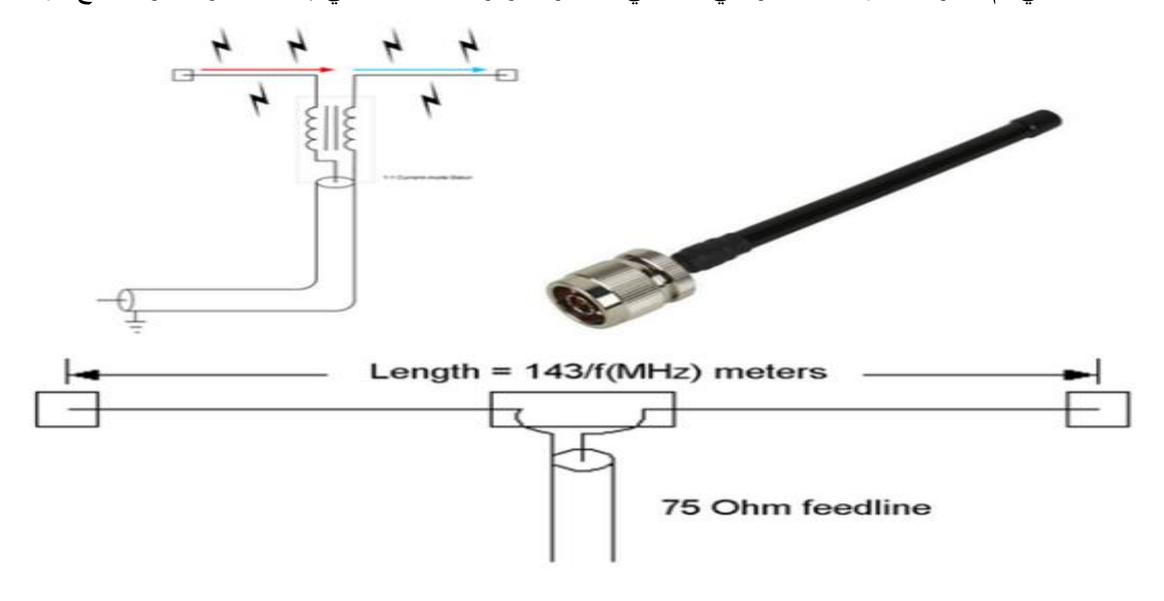
هذه الهوائيات شاملة لكل الاتجاهات تشع الطاقة الكهرومغناطيسية بشكل منتظم في جميع الاتجاهات. وعادة ما تشع موجات قوية بشكل موحد في بعدين. هذه الهوائيات هي فعالة في مناطق المحطات اللاسلكية التي تستخدم تكنولوجيا **time division multiple access**. وخير مثال على هذا هي تلك التي تستخدمها محطات الراديو. هذه الهوائيات فعالة لنقل إشارات الراديو لأن المتلقي قد لا يكون ثابت. لذلك، يمكن للراديو تلقي الإشارة بغض النظر عن أين هو.

- **Yagi Antennas**

يسمي أيضا **Yagi-Uda antennas** نسبة الي مخترعيه اليابانيين **Shintaro Uda** و **Hidetsugu Yagi** في عام 1926 وتم استخدامه علي نطاق واسع في الحرب العالمية الثانية في الرادارات المحمولة جوا و ذلك لبساطة تصميمه. وهو نفسه الهوائي الذي يستخدم مع أجهزة التلفاز والذي يستطيع أي شخص صنعه بالأعواد المعدنية ولأسباب جمالية فإن استخدامه في الشبكات اللاسلكية حتم وضعه في أنبوب لاسلكي مع ضبط ابعاده.
هو هوائي أحادي الاتجاه يشيع استخدامه في الاتصالات ذات نطاق التردد من 10 ميغا هرتز في **VHF وUHF**. تحسين كسب الهوائي وخفض مستوى الضجيج من إشارة الراديو هي المحور الرئيسي لهذا الهوائي. هو يتألف من **reflector**، **dipole**، وعدد من **directors**.

- **Dipole Antenna**

وهو من الهوائيات **Omnidirectional** والتي تبث موجاتها في كل الاتجاهات الأفقية ويستخدم في الشبكات اللاسلكية الداخلية وتراه غالبا في كروت الشبكة اللاسلكية أو الأكسس بوينت المستخدم في البيوت.
ويسمي **Dipole** أي ثنائي القطب لأنه يتكون داخليا من جزئيين معدنيين بينهما مسافة صغيرة يتم تطبيق جهد تردد الراديو بينهما فتتحول الإشارة الكهربية الي اشارة لاسلكية تنتشر من خلال هذين الموصلين – تستطيع رؤيتهما عند النظر الى نقطة الاتصال أسفل الهوائي-وهو أبسط الهوائيات العملية التي تم اختراعها بواسطة الفيزيائي الألماني الشهير هيرتز سنة 1886 في إحدى تجاربه الرائدة مع موجات الراديو.



- **Parabolic Grid Antenna**

الهوائي **parabolic grid antenna** قائم على مبدأ طبق الأقمار الصناعية بدون **solid backing**. بدلا من **solid backing** فهذا النوع من الهوائيات لديه شيء شبيه بالطبق الذي يتكون من شبكة مصنوعة من أسلاك الألمنيوم. ويمكن لهذه الهوائيات تحقيق مسافات طويلة جدا من بث الواي فاي من خلال الاستفادة من مبدأ تركيز شعاع الراديو عاليا. هذا النوع من الهوائي يمكن أن يستخدم لنقل الإشارات اللاسلكية الضعيفة ملايين الأميال.



Parabolic grid antennas تمكين المهاجمين من الحصول على أفضل جودة للإشارة مما يؤدى إلى مزيد من التنصت على البيانات، والمزيد من الاستخدام السيء لعرض النطاق الترددي، وارتفاع انتاج الطاقة التي لا غنى عنها في هجمات الحرمان من الخدمة "**DoS**" ورجل في المنتصف "**MINTM**". **Grid parabolic antennas** يمكنه التقاط إشارات واي فاي من مسافة 10 ميل. تصميم هذا الهوائي يحفظ الوزن والمساحة ولها القدرة على التقاط إشارات واي فاي التي هي إما أفقي أو عمودي الاستقطاب.

15.2 تشفير الشبكات اللاسلكية "WIRELESS ENCRYPTION"

التشفير اللاسلكي "**Wireless encryption**" هي عملية حماية الشبكة اللاسلكية من المهاجمين الذين يمكنهم جمع المعلومات الحساسة الخاصة بك عن طريق اختراق حركة مرور تردد الراديو "**RF**". يقدم هذا القسم فكرة عن مختلف معايير التشفير اللاسلكية مثل **WEP**، **WPA**، **WPA2**، وقضايا **WEP**، وكيفية كسر خوارزميات التشفير، وكيفية الدفاع ضد كسر خوارزمية التشفير.

أنواع التشفير "Types of wireless Encryption"

الهجمات على الشبكات اللاسلكية تتزايد يوما بعد يوم مع تزايد استخدام الشبكات اللاسلكية. ولذلك، تأتي من هذه التكنولوجيا الناشئة مختلف خوارزميات التشفير اللاسلكي التي تجعل الشبكة اللاسلكية امنه. خوارزمية التشفير اللاسلكي تملك العديد من المزايا ولكن أيضا العديد من العيوب. وفيما يلي خوارزميات التشفير اللاسلكي حتى الان:

- **WEP**: هو بروتوكول مصادقة عملاء الشبكة المحلية اللاسلكية (**WLAN**) وتشفير البيانات وهو من اقدم وأول مستويات الامن الخاصة بالشبكات اللاسلكية ولكنها الان أصبحت ضعيفة ويمكن كسرها بسهولة.
- **WPA**: هو بروتوكول مصادقة عملاء الشبكة المحلية اللاسلكية (**WLAN**) وتشفير البيانات متطور حيث يقوم باستخدام نظام التشفير **TKIP**، **AES**، و**MIC**. يستخدم التشفير **48-bit IV**، **32-bit CRC**، أو **TKIP** لأمان الشبكات اللاسلكية.
- **WPA2**: يستخدم **AES (128-bit)** ، **CCMP** من اجل تشفير الشبكات اللاسلكية.
- **WPA2 Enterprise**: هو عباره عن دمج معيار **EAP** مع التشفير **WPA**.
- **TKIP**: هو بروتوكول امنى يستخدم في **WPA** كبديل لـ **WEP**.
- **AES**: هو نوع التشفير **a symmetric-key encryption**، ويستخدم في **WPA2** كبديل لـ **TKIP**.
- **EAP**: يستخدم العديد من أساليب المصادقة، مثل **token cards**، **Kerberos** و**certificates** وما إلى ذلك.
- **LEAP**: بروتوكول مصادقة **WLAN** والتي قامت بتكويرها شركة **Cisco**.
- **RADIUS**: خادم مركزي لإدارة المصادقة والتعريف "centralized authentication and authorization management system".

- **802.11i**: هو معيار **IEEE** والذي يحدد الآليات الأمنية للشبكات **802.11** اللاسلكية.
- **CCMP**: يستخدم المفاتيح **128-bit keys**، مع **48-bit initialization vector (IV)** من اجل **replay detection**.

تشفير WEP

مند ان ظهر الحاسوب ظهرت فكرة الربط بين حاسوب واخر مما ادى الى ظهور الشبكة والشبكة هي مجموعة من الحواسب المتصلة فيما بينها. في الاول كان الاتصال عن طريق الكابلات وبما ان هده الاخيرة مكلفة تم التفكير في الربط عن طريق الموجات اللاسلكية فهي اقل تكلفة ومن هنا أصبح لدينا نوعان من الشبكات شبكات سلكية وشبكات لاسلكية.
المشكلة تكمن في ان الشبكات اللاسلكية اقل حماية وهذا من طبيعتها اما الشبكات السلكية فهي أكثر حماية وهذا من طبيعتها فلكي يتمكن المخترق من الولوج الى الشبكة لابد له من وصل نفسه عن طريق الكابلات اما الشبكات اللاسلكية فيكفي ان يكون المخترق في مدار الشبكة حتى يتمكن من الولوج اليها.
في البداية كان كل من يكون في مدار الشبكة قادرا على الولوج اليها والتنصت على البيانات المارة فيها فتم التفكير في طريقة لتفادي هذه المشكلة فظهر بروتوكول **WEP = Wired Equivalent Privacy** والذي لديه الكثير من الثغرات الموجودة فيه حتى أصبح المخترقون يلقبونه بـ **Weak Encryption Protocol**. ظهر هدا البروتوكول اول مرة سنة 1999 في شبكات **802.11b** كوسيلة لحماية خصوصية البيانات **data confidentiality** التي تنتشر عبر الشبكات اللاسلكية ويعتبر بذلك أول وسيلة لتأمين الشبكات اللاسلكية.

ما هو تشفير WEP؟

على حسب موقع "http://searchsecurity.techtarget.com"هو بروتوكول امنى مخصص لشبكات الوايرلس وخاصة المعيار **IEEE 802.11b**. الغرض الرئيسي منه هو توفير سرية البيانات على الشبكات اللاسلكية على مستوى يعادل الشبكات السلكية. الأمان المادي يمكن تطبيقه في شبكات **LAN** السلكية لوقف الوصول الغير مصرح به إلى الشبكة.
في الشبكات اللاسلكية (**WLAN**) يمكن الوصول إليها من دون توصيل المادي بالشبكة كما في الشبكة السلكية. ولذلك، **IEEE** تستخدم آلية التشفير في طبقة **data link layer** لتقليل الوصول الغير مصرح به على شبكة **WLAN**. ويتم ذلك عن طريق تشفير البيانات مع خوارزمية التشفير **symmetric RC4 encryption algorithm**.

اهمية WEP في الاتصال اللاسلكي

- يحمي من التنصت على الاتصالات اللاسلكية.
- تقلل الوصول الغير مصرح به إلى الشبكة اللاسلكية.
- يعتمد على المفتاح السري. يتم استخدام هذا المفتاح لتشفير الحزم قبل الإرسال. المحطة ونقطة الوصول تتشاركان هذا المفتاح. من السلامة إجراء فحص للتأكد من أن الحزم (**packets**) لم يتغير أثناء الإرسال. **WEP 802.11** يقوم بتشفير البيانات فقط بين محطات **802.11**.

الأهداف الرئيسية

- السرية: يمنع التنصت.
- الوصول: يحدد من له الحق في الوصول إلى الشبكة، ومن ليس له الحق.
- تكامل البيانات: يحمي تغيير البيانات.
- الكفاءة.

تشفير WEP

لتشفير "**Encryption**" البيانات اللاسلكية. يستخدم **WEP** خوارزمية تدقيق **stream cipher** تسمي **Ron's Code 4 (RC4)** لتوليد بيانات مشفرة باستخدام **Key system** ويعتبر **RC4** خوارزمية متماثلة "**symmetric algorithm**" أي أن المفتاح المستخدم في التشفير عند المرسل هو نفسه المستخدم في فك التشفير عند المستقبل.
ينقسم **Key system** الي جزئيين أولهما هو **WEP Key** وهو رقم التشفير الذي تدخله في الجهاز والثاني هو **initialization vector (IV)** وهو رقم عشوائي خاص بعملية التشفير وطوله هنا **24bit** ويتم اضافته بشكل عشوائي الي **WEP Key** لتمويه **Key System** الذي ينقسم الي ثلاث أنوع وهم:

- **64-bit WEP uses a 40-bit key**
- **128-bit WEP uses a 104-bit key size**
- **256-bit WEP uses 232-bit key size**

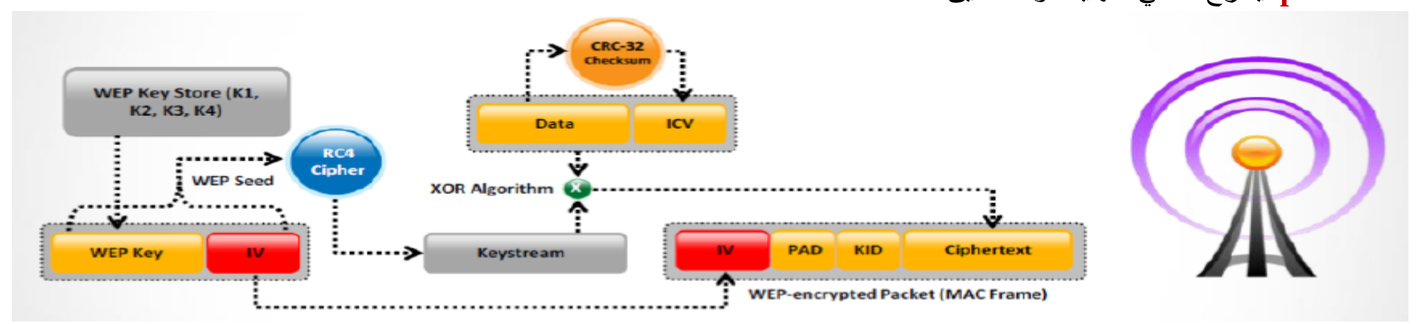


- **64-bit WEP** يسمي أيضا **(WEP-40)** لأنه يحتوي علي **10 byte hexadecimal** كل بايت يحتوي علي **4 bits** اي في النهاية **40 bit** ثم يتم اضافة **initialization vector (IV)** بطول **24 bit** لعمل **RC4** ليصل الي **64-bit WEP**. لكن الكثير من الأجهزة تجبرك على إدخال خمسة بيانات من النوع **ASCII** وهي بدورها تحول كل بيان حرف أو رقم الي ثمانية بت لتصل في النهاية الي **40 bit**.
- **128-bit WEP** يسمي أيضا **(WEP-104)** لأنه يحتوي علي **26 byte hexadecimal** كل بايت يحتوي علي **4 bits** اي في النهاية **104 bit** ثم يتم اضافة **initialization vector (IV)** بطول **24 bit** لعمل **RC4** ليصل الي **128-bit WEP**.
- **256-bit WEP** يسمي أيضا **(WEP-232)** لأنه يحتوي علي **58 byte hexadecimal** كل بايت يحتوي علي **4 bits** اي في النهاية **232 bit** ثم يتم اضافة **initialization vector (IV)** بطول **24 bit** لعمل **RC4** ليصل الي **256-bit WEP**.

ويتم التوزيع طبقا لنفس العملية الحسابية

(HEX × 4 bits = WEP key) + IV = WEP System

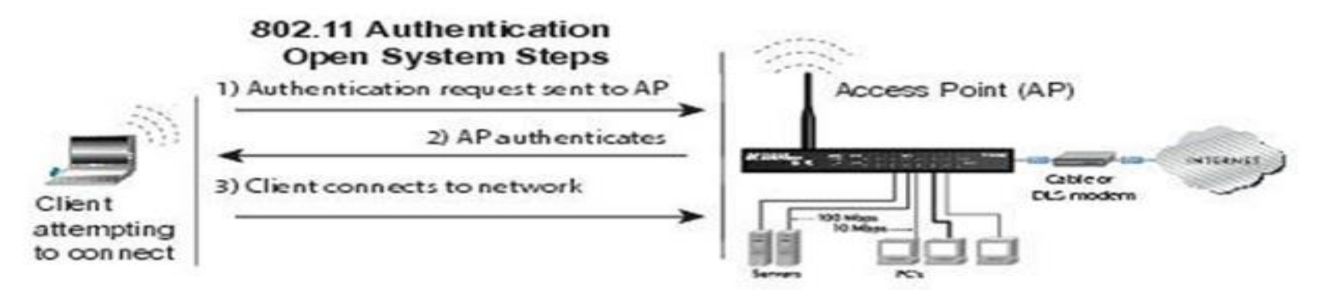
ويتم جمع **IV** مع **Key** ثم اضافة خوارزمية تدقيق **"stream cipher"** تسمي **RC4** لينتج **Keystream** ثم جمعها بطريقة **XOR** مع **plain text** ليخرج لنا في النهاية كود التدقيق.



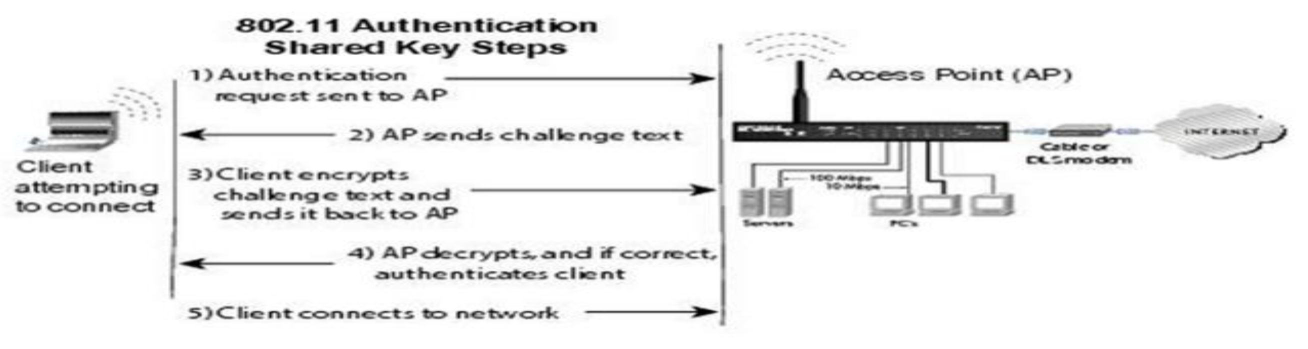
توثيق WEP

يتم استخدام نوعين من التوثيق "**Authentication**" مع **WEP** هما **Open System** و**Shared Key**.

أما **Open System authentication** لا يحتاج مستقبل الإشارة أي ترخيص لاستقبالها ويستطيع أي أحد أن يدخل الي الشبكة عبر الأكسس بوينت بما يسمي عملية الارتباط **Associate** ويستخدم هنا **WEP** فقط في تشفير البيانات المرسلة كي لا تري من الأشخاص خارج الشبكة.



وأما **Shared Key authentication** فيتم استخدام مفتاح **WEP** للتوثيق والتشفير على أربع خطوات أولها تقوم محطة العميل بإرسال طلب توثيق لدخول شبكة الأكسس بوينت يقوم بعدها الأكسس بوينت بالرد برسالة غير مشفرة تسمي **clear-text challenge** تقوم محطة العميل بعد استلام الرسالة بتشفيرها باستخدام مفتاح **WEP** ثم يرسلها للأكسس بوينت يقوم الأكسس بوينت بعد استلام الرسالة فإذا نجح في فك تشفيرها **decrypt** باستخدام مفتاح **WEP** فيتم السماح للجهاز بالولوج للشبكة.



ان كنت تظن أن هناك فرق بين الإثنين في مستوي الأمان وأن **Shared Key authentication** أوثق وأكثر أمانا فأنت مخطئ فكلا من الطريقتين سهل اختراقها أو أن أحدهما فقط أسهل من الأخرى فباستخدام برامج التقاط وتحليل الإشارة لرسالة **clear-text challenge** ايابا وذهابا من محطة العميل أي قبل وبعد التشفير يتم معرفة خوارزمية التشفير وفك رموزه أي أن في كل الأحوال **WEP** ضعيف.

عيوب WEP

- طرق التشفير التي تعتبر بدائية تستخدم خوارزمية خطية **Linear Checksum** أي أن تسلسل التشفير معكوس تسلسل فك التشفير بالضبط كأنك تقوم بتغليف علبة هدايا وهذه هي أسوأ عيوب **WEP**.
- كذلك في طرق التشفير يستخدم مفتاح أساسي **Key** و في **WEP** يتم اضافة بيانات عشوائية **IV** اليه كي لا يستطيع أحد فهم طريقة التشفير و تسمي البيانات العشوائية **24 bit** و رغم أن هذه البيانات عشوائية يصعب توقعها الا أنها بيانات **plain text** أي مقروءة بالإضافة الي أنها ليست بالطول الكافي فيمكن تكرار نفس **IV** بعد ارسال 5000 حزمه و لهذا عند استخدامك برنامج **air crack** في كالي لينكس و ما يشبهها تلاحظ أنك عند استخدام أمر كسر الحزمة **aircrack-ng** فأنه ينبهك الي الانتظار بعد قراءة 5000 حزمه أو مضاعفاتها اذا لم يكن قادرا بعد علي الكسر و عموما لا يستغرق هذا الأمر كله أكثر من نصف ساعة. و يعتبر أول من أثبت امكانية كسر **WEP** هو العالم الإسرائيلي **Adi Shamir** بمساعدة آخرين و هم **Scott Fluhrer, Itsik Mantin** في August 2001 أي لم يكن **WEP** قد أتم عامه الثاني بعد ثم تباري العلماء و المتخصصون بعدهم في كسره في أقل وقت
- كذلك بمجرد معرفة **WEP Key** فإنك تستطيع الولوج ومشاركة الآخرين بنفس **KEY** على عكس بعض تقنيات التشفير الأخرى التي حتى وإن عرفت **Key** فلابد من وسيلة لتوثيق دخولك الشبكة.

تخطى العيوب

تم تطوير **WEP** في السنوات الأخيرة وادخال تحسينات عليه من قبل **Agere Systems** وذلك عبر تخطي عيوب **IV** وسمي بعدها باسم **WEP Plus** الا أن ظهور **WPA** قد حد من انتشاره

كذلك ظهر تحسين آخر سمي بـ **Dynamic WEP** وهو مزج بين تقنيتي **802.1X** و**EAP Extensible Authentication Protocol** وقام بتغيير دوري في **WEP Key** ولكن هذا التحسين كان حصري فقط لشركة **COM3**.

المصدر: http://wireless4arab.net **للكاتب نادر المنسي.**

تشفير WPA

نظرا لضعف تقنية التشفير **Wired Equivalent Privacy (WEP)** فقد قامت مؤسسة **Wi-Fi** و**IEEE** بالعمل سويا لاستبداله بمعيار أكثر أمانا وخرج الي النور جيلين الأول يخص **Wi-Fi** وهو **Wi-Fi Protected Access (WPA)** والثاني يخص **IEEE** ويسمي **IEEE 802.11i/WPA2**.

فأما **Wi-Fi Protected Access (WPA)** فقد قامت منظمة الواي فاي بإطلاقه في 2003 بغرض سرعة استبدال المعيار القديم **WEP** وهو النسخة الأولية **draft** للمعيار الأحدث **Wi-Fi Protected Access II (WPA2)** والذي يسمي أيضا **IEEE 802.11i**.

يمثل **WPA** الوصول المحمي الى شبكة الواي فاي. وهو متوافق مع **802.11i**. في الماضي آلية الامن الاولية المستخدمة بين نقاط الوصول اللاسلكي هو تشفير **WEP**. وكان العيب الرئيسي في تشفير **WEP** هو أنها لا تزال تستخدم مفتاح تشفير ثابت. يمكن للمهاجم استغلال هذا الضعف باستخدام أدوات متاحة مجانا على شبكة الإنترنت. ولذلك قامت جمعية مهندسي الكهرباء والإلكترونيات **(IEEE)** "بتوسيع بروتوكول 802.11 والتي يمكن أن يسمح بمزيد من الأمان".

لقد تم زيادة معايير تشفير البيانات والامن في **WPA** حيث يتم تمرير الرسائل عبر **Message Integrity Check (MIC)** باستخدام بروتوكول **Temporal Key Integrity Protocol (TKIP)** وذلك لتعزيز تشفير البيانات.

إذا تكمن فكرة **WPA** في استخدام **Temporal Key Integrity Protocol (TKIP)** وذلك لتغيير مفاتيح التشفير بطول **128-bit** بشكل اوتوماتيكي لكل **Packet** على عكس **WEP** الذي يستخدم مفاتيح تشفير بطول **40-bit** أو **104-bit** تدخلها في الأكسس بوينت والجهاز الذي سيستخدم الشبكة والذي يستخدم تقنية **RC4** وتم بعدها تعديل بنيته ليعتمد على **AES encryption**. يحتوي أيضا **WPA** على تقنية تسمي **Micheal** وهي تقنية فحص الحزم **MIC** وهي البديلة لتقنية **cyclic redundancy check (CRC)** المستخدمة في **WEP** وهذه التقنية هي التي مكنت **WPA** من منع اختراقه بحجب عملية **capturing** التي تستخدم في أخذ نسخ من الحزم المرسلة وتحليلها لاختراق الشبكة ورغم قوة **MIC** الا أنه استبدل ايضا في **WPA2** بوسيلة أكثر قوة.

- **Temporal Key Integrity Protocol (TKIP)**: **TKIP** يستخدم الإصدار **RC4 stream cipher encryption** مع المفتاح **128-bit** والمفاتيح **64-bit** وذلك للمصادقة. **TKIP** يخفف الضعف في مفتاح **WEP** مع عدم إعادة استخدام نفس **IV**.

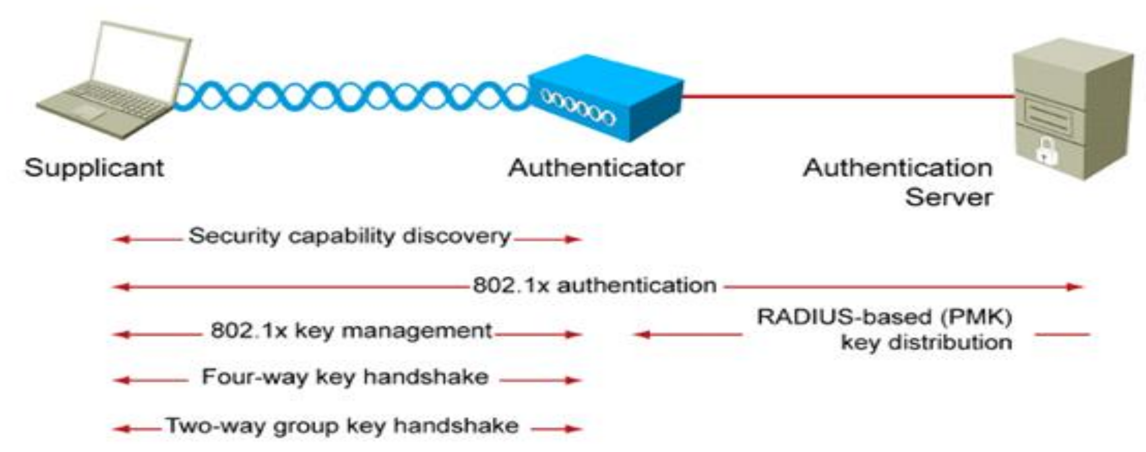
- **128-bit Temporal Key**: تحت **TKIP**، العميل يبدأ مع **128-bit Temporal Key (TK)** ثم يتم ربطه مع عنوان MAC الخاص بالعميل ثم مع **IV** لإنشاء مفتاح يستخدم لتشفير البيانات عبر **RC4**. ومن ثم يقوم بتنفيذ **sequence counter** للحماية ضد هجمات إعادة التشغيل.
- **WPA Enhances WEP**: **TKIP** يعزز **WEP** بإضافة آلية **rekeying mechanism** لتوفير مفاتيح تشفير جديده. يتم تغيير **Temporal Key** لكل 10,000 من الحزم. هذا يجعل **TKIP** الشبكات محمية أكثر ومقاومة.

WPA Authentication Modes

Enterprise (802.1X Authentication)	Personal (PSK Authentication)
Authentication server required	Authentication server not required
RADIUS used for authentication and key distribution	Shared secret used for authentication
Centralized access control	Local access control
Encryption uses TKIP, AES optional	Encryption uses TKIP, AES optional

لدينا نوعان من التوثيق هما (**WPA Personal**) و (**WPA Enterprise**).

- في **WPA Personal** يتم استخدام مفتاح متفق عليه بين الجهاز والأكسس بوينت (**(WPA-PSK) pre-shared keys**) وهو المستخدم غالبا في الشبكات الخفيفة **SOHO** مثل المنازل حيث يعتبر استخدام **RADIUS server** خيار غير عملي ولهذا فإن **WPA** يشبه **WEP** في كونه يسمح باستخدام **pre-shared key (PSK)** كمفتاح مشترك بين **client** و**access point**.
- في **WPA Enterprise** يتم استخدام سيرفر مركزي ببروتوكولات توثيق **802.1X/EAP** أو بأي نوع **EAP** مثل **EAP-TLS (Transport Layer Security)** أو **EAP-TTLS PEAP (Protected EAP)** أو [**Microsoft Challenge Handshake Authentication Protocol**] **MS-CHAP v2** أو غيرها.



كما هو الحال مع بروتوكولات التوثيق يتم استخدام فريمات التراسل (**probe request, probe response**) بين الجهاز و الأكسس بوينت الا أن الاختلاف يكمن في أنه لابد أن يتوافق الأكسس بوينت و الجهاز علي هذه العملية أمنيا ثم يستكمل خطوات توثيق **802.1x** وعند استكمالها يقوم السيرفر بإرسال **master key** الي الأكسس بوينت و التي أخذها مسبقا من الجهاز الطالب للاتصال و لهذا يسمي المفتاح **Pairwise Master Key (PMK)**.

ثم يتم بعدها عملية تراسل رباعي **four-way handshake** والتي يتم منها توليد مفتاح آخر يسمي **Pairwise Transient Key (PTK)**.

ثم يبدأ بعدها مرحلة جديدة من التراسل تسمي **two-way group key handshake** يحدث تراسل مشفر بواسطة **Group Transient Key (GTK)**، بين **client** و **authenticator**.

Unicast Keys: Four-Way Handshake

يتم التراسل بين الأكسس بوينت عبر أربع خطوات تسمي **four-way handshake** ينتج بعدها مفتاح جديد يسمى **Pairwise Transient Key (PTK)** يؤكد عملية الاتصال والتي بدأت عبر المفتاح **Pairwise Master Key (PMK)**.

عملية التراسل WPA four-way الرباعي عدة فوائد أهمها

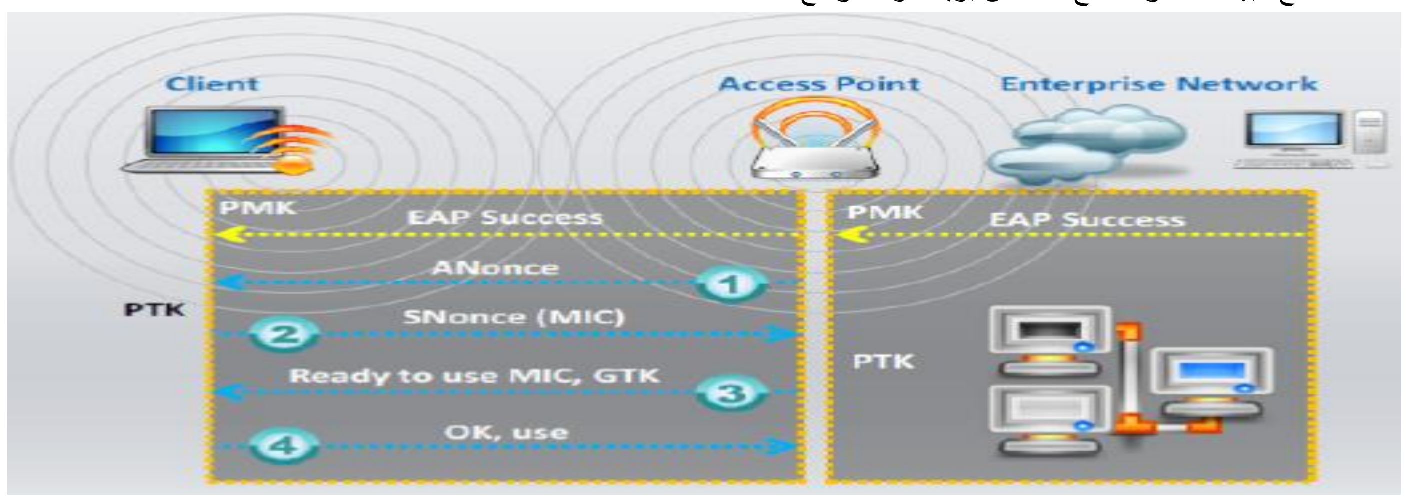
- تأكيد المفاتيح PMK بين Supplicant و Authenticator
- توليد المفاتيح المؤقتة pairwise temporal keys
- توثيق معاملات التأمين المتبادلة.

قبل أن تحدث عملية التراسل الرباعي **WPA four-way handshake** لابد أن يتم توليد **pairwise master key** كنتيجة لعملية توثيق **802.1x** بين **client** و**authentication server** ثم تتوالى الخطوات التالية

- أولا يقوم **AP** بإرسال رقم عشوائي **Nonce** الي محطة العميل ويستخدم لجلسة واحدة فقط **one session**.
- ثانيا بهذا الرقم العشوائي وباستخدام أيضا **PMK** تقوم محطة العميل بتوليد مفتاح لتشفير البيانات التي سترسل الي **AP** ويتم استخدام دالة تسمي **pseudo-random function (PRF)** وذلك لحساب **PTK** كدالة في الأرقام العشوائية المتولدة في محطة العميل و**AP** وفي **MAC** وفي **PMK** أو المفتاح المشترك ويتم حماية **frame** المرسل بواسطة **frame check sequence (FCS)** بواسطة تقنية **message integrity check (MIC)** وذلك للتأكد من أن **frame** لم يتم اعتراضه.
- ثالثا يقوم الأكسس بوينت بعد تلقيه **nonce** بإرساله مرة اخري الي **Client** بنفس السياسة الأمنية المستقبل بها ويقوم أيضا الأكسس بوينت بإرسال **group key** وبهذا يكون هناك توثيق بين الأكسس بيونت والجهاز.
- رابعا يتم تأكيد أن المفاتيح قد تم ارسالها والعملية جاهزة للتراسل.

بمجرد الحصول على المفتاح المؤقت PTK بطول 64-bit فإنه يتم تقسيمه الي خمس مفاتيح

- الأول بطول **16-byte** ويسمي **EAP over LAN-Key Encryption Key** ويختصر لـ **EAPOL-KEK** ويستخدم في تشفير أي بيانات إضافية مرسلة الي **Client**.
- الثاني بطول **16-byte** ويسمي **EAPOL-Key Confirmation Key** ويختصر لـ **KCK** ويستخدم لحساب **MIC**.
- الثالث بطول **16-byte** و هو **Temporal Key TK** ويستخدم لتشفير وفك تشفير **unicast data Packets**
- الرابع والخامس كل منهما بطول **8-byte** و هما **Michael MIC Authenticator** وأحدهما يستخدم لحساب **MIC** المرسل مع البيانات المرسلة مع الأكسس بوينت والآخر مع **Client**.



Group Key Handshake

يستخدم **GTK (GroupWise Transient Key)** لمنع الجهاز من استقبال أي رسائل من الأكسس بوينت ويتم ذلك عبر التراسل الثنائي **two-way handshake** بهذا السيناريو:

- أولا يقوم الأكسس بوينت بإرسال **GTK** جديد لكل الأجهزة في الشبكة ويتم تشفيرها باستخدام **KEK** وحمايتها باستخدام **MIC**.
- ثانيا تقوم هذه الأجهزة بالاستجابة لـ **GTK** والرد على الأكسس بوينت.

ويكون GTK (GroupWise Transient Key) بطول 32-byte مقسمة الي ثلاث مفاتيح

- الأول بطول **16-byte** و هو **Temporal Key TK** ويستخدم لتشفير وفك تشفير **unicast data packet**.

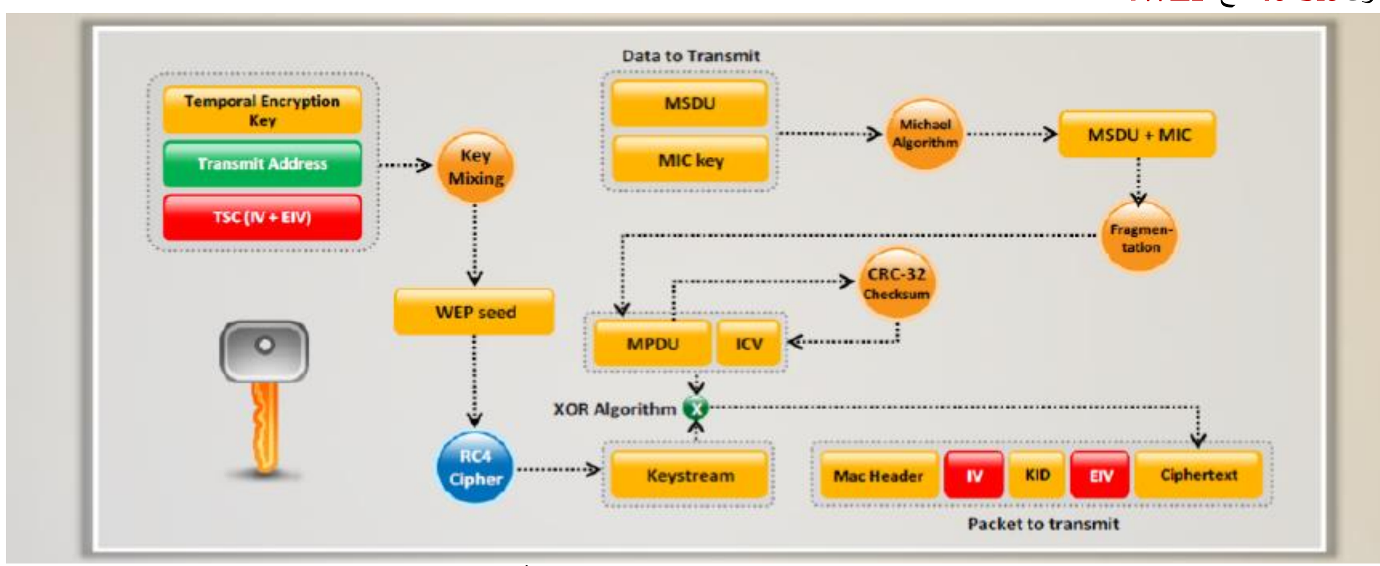
- الثاني والثالث كل منهما بطول **8-byte** وهما **Michael MIC Authenticator** وأحدهما يستخدم لحساب **MIC** المرسل مع البيانات المرسلة مع الأكسس بوينت والآخر مع **Client**.

WPA Encryption

كما أن **WPA** قد دعم عملية التوثيق **authentication** بشكل كبير فإنه أيضا فد قام بتحسين التشفير **encryption** أيضا بشكل رائع حسن وذلك عبر نظامين هما **AES** و**TKIP**.

أما **AES** فهو نظام جديد أقوي من نظام التشفير **RC4** المستخدم مع **WEP** ولكنه يحتاج الي الكثير من الطاقة بالإضافة الي ضرورة دعم الجهاز لهذا النوع من التشفير

وأما **TKIP** وهو اختصار **Temporal Key Integrity Protocol** فهو بروتوكول لا زال يستخدم تقنية **RC4** وهو الخيار الافتراضي لـ **WPA** الا أن به تحسينات عن الذي يستخدم مع **WEP** حيث أنه يستخدم مفاتيح بطول **128-bit** بعد أن كان يستخدم مفاتيح بطول **40-bit** مع **WEP**.

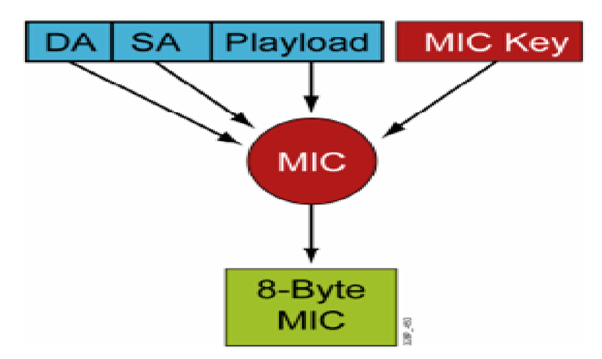


أما العيب الثاني الذي تخطاه **WPA** هو **IV initialization vector** فمن المعروف أن المفتاح يتم مزجه مع المفتاح الرئيسي بواسطة عملية **XOR** كما بالشكل السابق ولأن **IV** في **WEP** قيمة محددة لا تتغير وغير مشفرة فإنه وباستخدام بعض برامج تحليل **Packets** تستطيع أن تكشف قيمة **IV** ومن ثم كسر هذا التشفير وذلك في غضون ساعات قليلة.

أما في **WPA** فتغيرت هذه العملية كذلك أصبح **IV** بطول **48-bit** وليس بطول **24-bit** كما كان في **WEP** وهذا يحتاج **280** تريليون محاولة لكسره أي ما يساوي محاولات تتم في 645 سنة.

كذلك يتم عمل عملية مزج لكل من مفتاح **PTK** مع عنوان الجهاز **MAC** مع رقم كل حزمه مخرجا لنا مفتاح متغير لكل حزمه ثم مزج ذلك مع **IV** ليتم تشفير البيانات المرسلة بها وبهذا فإنه بالإضافة لصعوبة كسر هذا التشفير فإنه الأكسس بوينت يستطيع اكتشاف عملية الاختراق بواسطة عنوان الجهاز المرسل مع مفتاح التشفير.

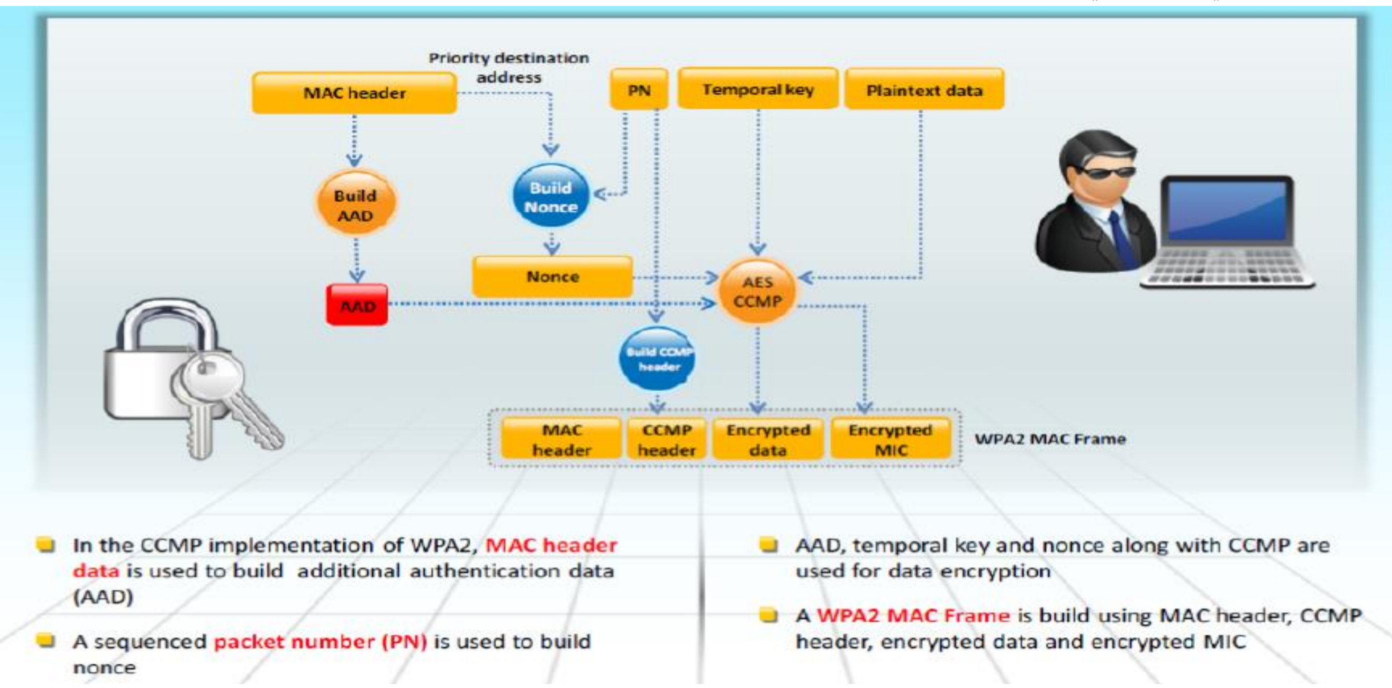
<u>Message Integrity Check</u>



التعديل الآخر في **WPA** هو استخدام تقنية تسمي **Message Integrity Code** تختصر الي **MIC** أو **Michael** حيث يتم وضع بعض **bits** القليلة الي الحزمة قبل تشفيرها وذلك لمراقبة مدي سلامة ارسال الحزمة.

WPA2 / 802.11i

الآن لدينا في **WPA** مفاتيح أطول و**IV** أطول ومزج فعال وكذلك تقنية **MIC** للتأكد من سلامة وصول الحزمة "**packet**" الا أن عملية التراسل الرباعي الموجودة في **WPA PSK** المدعوم افتراضيا في الشبكات تغري بالاختراق وذلك عبر عمل عملية فك الارتباط **deauthentication** ومن ثم انتحال شخصية أحد أجهزة الشبكة، وان كان هذا الأمر أصعب بكثير مما يتم في **WEP** الا أنه يحدث وهذا ما دعا الخبراء الي الانتقال الي **WPA2**.



WPA2 مبني علي **802.11i** وانتهي منه في 2004 و يدعم بروتوكولات التوثيق المركزي **802.1x** وفيه استبدل تقنية التشفير **RC4** بالجيل الثاني من طرق التشفير **AES** الذي أطلق من قبل **National Institute of Standards and Technology (NIST)** والذي يستخدم في عمليات المزج تسمي **Rijndael algorithm**.

تطوير سيسكو الخاص بـ WPA

دائما سيسكو لها لمساتها في أي تقنية ومن هذه اللمسات الرائعة **key caching** حيث يتم حفظ مفاتيح الولوج عند خروج الأجهزة من الشبكة وذلك عبر تثبيت قيمة **SA** لكل جهاز وعند رجوعه الي حيز الشبكة يستطيع الدخول مرة أخري بدون الحاجة الي إعادة التوثيق. كذلك قامت سيسكو بتطوير **WPA** بعمل مركزية لمفاتيح الولوج تسمي **Cisco Centralized Key Management** حيث يقوم الكنترولر بإدارة عمليات الربط **association** كما يحدث في **802.1x** حيث يقوم الكنترولر بدور الموثق **authenticator** وليس الأكسس بوينت فبمجرد ارتباط الأكسس بيونت بالكونترولر يتم توثيقه في أقل من 100 مللي ثانية ويحدث نفس الأمر عند رجوعه مرة أخري في حال ابتعاده حيث يحدث تخزين **caching** لمفتاح **PMK**.

WEP VS. WPA VS. WPA2

ان الهدف الرئيسي من **WEP** هو توفير سرية البيانات على الشبكات اللاسلكية على مستوى يعادل شبكات **LAN** السلكية، ولكنها ضعيفة ولا تستوفي أي من أهدافها. وهي طريقة تشفير البيانات للشبكات اللاسلكية **802.11**. **WPA** قامت بإصلاح معظم مشاكل **WEP** ولكنها اضافت ثغرات جديده. **WPA2** يتوقع من أن يجعل الشبكات اللاسلكية آمنة كالشبكات السلكية. وتضمن الشبكة أن المستخدمين المرخص لهم فقط يمكنهم الوصول إلى الشبكة. إذا كنت تستخدم **WEP**، فيجب استبداله مع إما **WPA** أو **WPA2** من أجل تأمين شبكتك أو الاتصال على شبكة **Wi-Fi**. كلا **WPA** و**WPA2** تتضمن الحماية ضد التزوير وتكرار الهجمات.

Encryption	Attributes			
	Encryption Algorithm	IV Size	Encryption Key Length	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bit	CRC-32
WPA	RC4, TKIP	48-bit	128-bit	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bit	128-bit	CBC-MAC

WEP	Should be replaced with more secure WPA and WPA2
WPA, WPA2	Incorporates protection against forgery and replay attacks

قضايا الـ WEP "WEP ISSUES"

WEP، يملك بعض من القضايا التالية:

1- CRC32 لا تكفي لضمان سلامة التشفير الكامل للحزمة:

عند التقاط اثنين من الحزم، يمكن للمهاجم **reliably flip a bit** في التشفير، ومن ثم تعديل **checksum** فتصبح الحزمة مقبلوه.

2- IVs are 24 bits :

AP يمكنها بث **1500-byte** من الحزم بمعدل 11 Mb/s والذى يؤدى الى استنفاذ لمساحة **IVs** في خمس ساعات.

3- Known plaintext attacks :

عندما يكون هناك **IV collision** فقد يصبح من الممكن إعادة بناء **RC4 keystream** القائم على **IV** ومن ثم فك تشفير الحزمة.

4- Dictionary attacks:

WEP قائمه على كلمة مرور.

المساحة الصغيرة لـ **IV** يسمح للمهاجم إنشاء وفك تشفير الجدول، وذلك باستخدام هجوم القاموس.

5- الحرمان من الخدمة:

لا يتم مصادقة **Associate and disassociate messages**.

6- في نهاية المطاف، يمكن للمهاجم بناء جدول التشفير من إعادة ترميز الجداول الرئيسية:

24-جيجابايت من المساحة، يمكن للمهاجم استخدام هذا الجدول لفك تشفير **WEP** في الوقت الحقيقي.

7- عدم وجود centralized key management يجعل من الصعب تغيير مفاتيح WEP مع أي انتظام

8- IV هي القيمة المستخدمة لعشوائية "randomize" قيمة مفتاح key stream لذلك كل حزمه لها قيمة IV.

كيفية كسر تشفيرWEP ؟

لكسر مفتاح تشفير **WEP** فمن الضروري جمع بعض من **IVs**. المهاجم يقوم بجمع **IVs** المناسب لكسر مفتاح **WEP** وذلك من خلال الاستماع إلى حركة مرور الشبكة وحفظها. الحقن "**Injection**" يمكن استخدامه لتسريع عملية جمع **IVs**. الحقن "**Injection**" يسمح بالاستيلاء على عدد كبير من **IVs** في فترة قصيرة من الوقت. لكسر تشفير **WEP** فان المهاجم يتبع الخطوات التالية:

- بداية قم بتحويل وضع واجهة الشبكة اللاسلكية "**Wireless Interface**" الى وضع المراقبة "**monitor mode**" على قناة **AP** المحددة.

في هذه الخطوة يقوم المهاجم بتحويل وضع كارت الشبكة اللاسلكية الى الوضع **Monitor Mode**. في هذا الوضع فان واجهة الشبكة يمكنها الاستماع إلى كل حزمة في الهواء. المهاجم يمكنه تحديد بعض الحزم للحقن وذلك من خلال الاستماع إلى كل الحزم في الهواء.

- اختبار القدرة على الحقن من قبل الجهاز اللاسلكي الى **AP**.

هنا المهاجم يختبر الواجهة اللاسلكية ما إذا كانت ضمن نطاق **AP** وايضا المقدرة على حقن الحزم اليها.

- استخدام أداة مثل **aireplay-ng** لأداء مصادقة زائفه مع **AP**.

هنا المهاجم يجب أن يتأكد أن عنوان **MAC** المصدر مقترن بالفعل فيصبح عند حقن الحزمة مقبول من قبل **AP**. الحقن يفشل بسبب عدم وجود رابط مع **AP**.

- بدء استخدام أداة التنصت على الواي فاي.

في هذه الخطوة يجب على المهاجم التقاط **IVs** الناشئة وذلك باستخدام أدوات مثل **airodump-ng** مع الفلتر **bssid** وذلك لجمع IVs الفريد.

- البدء في استخدام أداة تشفير حزم الواي فاي مثل **aireplay-ng** في طلب **ARP** في الوضع **replay mode** وذلك لحقن الحزم.

المهاجم يجب أن يحصل على عدد كبير من **IVs** في فترة قصيرة من الوقت. وهذا يمكن أن يتحقق من خلال تشغيل **aireplay-ng** في طلب **ARP** في الوضع **replay mode** والذي فيه يستمع إلى طلبات **ARP** ومن ثم إعادة حقنهم في الشبكة. **AP** عند اعادة بث الحزم يقوم بإنشاء **IV** جديدة. لذلك من أجل كسب عدد كبير IVs فان المهاجم يختار الوضع **ARP replay mode**.

- تشغيل أداة المسر مثل **Cain & Abel** أو **aircrack-ng**.

باستخدام أدوات فك التشفير مثل **Cain & Abel** أو **aircrack-ng** فان المهاجم يمكنه استخراج مفاتيح تشفير **WEP** من IVs.

كيفية كسر تشفير WPA؟

تشفير **WPA** هو أقل ضعفا بالمقارنة مع تشفير **WEP**. **WPA/WPA2** يمكن أن يتم كسره بعد الاستيلاء على النوع الصحيح من الحزم. الكسر يمكن ان يتم في الوضع **offline** ويحتاج ان يكون بالقرب من **AP** للحظات قليله.

- **WPA PSK**

هنا يستخدم كلمة المرور المستخدم وذلك لتهيئة **TKIP**، والذي هو غير قابل للكسر كما انه **Pre-Packet Key** ولكن المفتاح يمكن يكسر من خلال استخدام هجمات القاموس.

- **Offline Attack**

لتنفيذ هجوم **Offline Attack**، فما عليك إلا أن تكون قريبا من **AP** لعدة ثوان من أجل التقاط **WPA/WPA2 authentication handshake**. بعد الاستيلاء على النوع الصحيح من الحزم، فيمكن كسر مفاتيح تشفير **WPA** في الوضع **offline**. كلمة مرور **WPA handshake** لا ترسل عبر الشبكة في حين ان **WPA handshake** تحدث عبر قنوات غير آمنة، في نص عادي. التقاط **authentication handshake** كامل من العميل ونقطة الوصول تساعد في كسر تشفير **WPA/WPA2** من دون حقن أي حزمة.

- **De-authentication Attack**

لأداء هجوم **de-authentication attack** من أجل كسر تشفير **WPA**، فإنك حاجة الى عميل مرتبط بالفعل بالشبكة. ثم اجبار العميل المتصل بالانفصال عن الشبكة ومن هنا تقوم بالتقاط حزم إعادة الاتصال والمصادقة باستخدام ادوات مثل **airplay**، ينبغي أن تكون قادرًا على إعادة المصادقة في بضع ثوان ثم محاولة هجوم القوة الغاشمة على **PMK**.

- **Brute-Force WPA Keys**

تقنية القوة الغاشمة "**Brute-Force**" يمكن استخدامها لكسر مفتاح تشفير **WPA/WPA2**. ويمكن أداء هذا الهجوم من خلال استخدام **Dictionary**. أو يمكن أن يتم ذلك باستخدام أدوات مثل **aircrack**، **airplay**، أو **KisMmac**. كسر تشفير **WPA** باستخدام تقنية القوة الغاشمة قد يستغرق ساعات او ايام او حتى اسابيع.

15.3 التهديدات المحتملة على الشبكات اللاسلكية "WIRELESS THREATS"

حتى الآن، قد ناقشنا مختلف مفاهيم الواي فاي وآليات الأمن مثل خوارزميات التشفير. الآن سوف نناقش المخاطر الأمنية المرتبطة بالشبكات اللاسلكية.

يتناول هذا القسم مختلف التهديدات والهجمات على الشبكات اللاسلكية مثل **rogue access point attacks**، **client mis-association**، وهجمات الحرمان من الخدمة "**DoS**"، وما إلى ذلك.

التهديدات المحتملة على الشبكات اللاسلكية: هجمات التحكم في الوصول "Access Control Attack"

هجمات التحكم في الوصول "**Access Control Attack**" تهدف إلى اختراق الشبكة بالتهرب من تدابير الرقابة الخاصة بالتحكم في الوصول الى الشبكة اللاسلكية، مثل **AP MAC filters** و**Wi-Fi port access controls**. هناك أنواع عديده من هجمات التحكم في الوصول. وفيما يلي أنواع لهجمات التحكم في الوصول إلى شبكات الوايرلس:

Wardriving

في هجوم **Wardriving**، يتم الكشف عن الشبكة اللاسلكية لاسلكية (**wireless LANS**)، أما عن طريق إرسال **probe requests** (طلبات التحقق) من خلال الاتصال أو عن طريق الاستماع إلى البرامج الملحقة للتتبع على الويب (**web beacons**). بمجرد اكتشاف نقطة الاختراق، فيمكن شن هجمات على الشبكة المحلية. بعض من الأدوات التي يمكن أن تستخدم لأداء **Wardriving** هي **KisMAC** و**NetStumbler** و**WaveStumber**.

ملحوظه: منارات الشبكة Web Beacons او التي يطلق عليها في بعض الأحيان Web bug، او pixel tag، او clear GIF، او صور gif أحادية البيكسل، وهذه عادة ما تستخدم مع الكوكيز. Web Beacons هي صورة بيانية في كثير من الأحيان شفافة، وعادة لا يزيد حجمها عن 1 بيكسل × 1 بيكسل، التي يتم وضعها على موقع على الانترنت أو في البريد الإلكتروني الذي يستخدم لمراقبة سلوك المستخدم من زيارة موقع ويب أو إرسال البريد الإلكتروني.

Rogue Access Points

من اجل إنشاء **backdoor** في شبكة اتصال موثوق به، يتم تثبيت نقطة وصول غير امنه أو نقطة وصول مزيفه داخل جدار حماية. أي من برمجيات أو أجهزة نقطة الوصول تستعمل لأداء هذا النوع من الهجوم.

MAC Spoofing

باستخدام تقنيات **MAC Spoofing**، يمكن للمهاجم إعادة تكوين عنوان **MAC** لظهر كنقطة وصول مأذون بها إلى المضيف على شبكة اتصال موثوق بها. الأدوات اللازمة للقيام بهذا النوع من الهجوم: **changemac.sh**، **SMAC**، و**Wicontrol**.

Ad Hoc Associations

هذا النوع من الهجوم يمكن القيام به باستخدام أي **USB adapter** أو بطاقة لاسلكية (**wireless card**). في هذا الأسلوب، المضيف يتصل إلى محطة غير امنه لشن هجوم على محطة معينة أو تجنب الوصول إلى نقطة الأمان.

AP Misconfiguration

إذا كان أي من إعدادات الأمان الحرجة مكونه بشكل غير صحيح في أي من نقاط الوصول، فيمكن أن تكون شبكة الاتصال بأكملها مفتوحة لنقاط الضعف والهجمات. لا يمكن تشغيل تنبيهات **AP** في معظم نظم كشف التسلل، كما أنها مخولة كجهاز مشروع على الشبكة.

Client Misassociation

جهاز العميل قد يتصل أو يقترن بنقطة الوصول (**AP**) من خارج الشبكة المشروعة أما عن قصد أو عن غير قصد. وهذا يرجع إلى أن إشارات الشبكات اللاسلكية (**WLAN signals**) تتنقل من خلال الجدران في الهواء. هذا النوع من **Client Misassociation** يمكن أن يؤدي إلى هجمات التحكم في الوصول.

Unauthorized Association

الوصول الغير مصرح به (**Unauthorized Association**) هو التهديد الرئيسي لشبكة الاتصال اللاسلكية. منع هذا النوع من الهجوم يعتمد على الأسلوب أو التقنية التي يستخدمها المهاجم من أجل الحصول على ارتباط مع الشبكة.

Promiscuous Client

Promiscuous Client يقدم إشارة قوية بشكل لا يقاوم من اجل الأغراض الخبيثة. وكثيراً ما تبحث البطاقات اللاسلكية على الإشارات الأقوى للاتصال بشبكة الاتصال. وبهذه الطريقة **Promiscuous Client** يجلب انتباه المستخدمين تجاهه عن طريق إرسال إشارة قوية.

التهديدات المحتملة على الشبكات اللاسلكية: الهجمات على السلامة (Integrity Attacks)

في هذا النوع من الهجمات يرسل المهاجم تحكم، إدارة أو إطارات البيانات مزوره او وهميه عبر شبكة اتصال لاسلكية وذلك لإعادة توجيه الأجهزة اللاسلكية من أجل القيام بنوع آخر من الهجوم (مثل **DOS**).

Type of attack	Description	Method and Tools
Data Frame Injection	Crafting and sending forged 802.11 frames.	Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject
WEP Injection	Crafting and sending forged WEP encryption keys.	WEP cracking + injection tools
Data Replay	Capturing 802.11 data frames for later (modified) replay.	Capture + injection tools
Initialization Vector Replay Attacks	The key stream is derived by sending the plain-text message.	
Bit-Flipping Attacks	Captures the frame and flips random bits in the data payload, modifies ICV, and sends to the user.	
Extensible AP Replay	Capturing 802.1X Extensible Authentication Protocols (e.g., EAP Identity, Success, Failure) for later replay.	Wireless capture + injection tools between station and AP
RADIUS Replay	Capturing RADIUS Access-Accept or Reject messages for later replay	Ethernet capture + injection tools between AP and authentication server
Wireless Network Viruses	Viruses have their impact on the wireless network to a great extent. It allows the attacker with simplest ways for attacking on APs.	

التهديدات المحتملة على الشبكات اللاسلكية: الهجمات على السرية (Confidentiality Attacks)

هذه الهجمات تحاول اعتراض المعلومات السرية المرسلة عبر النقاط اللاسلكية، سواء كان هذا الإرسال في نص واضح أو مشفر ببروتوكولات الواي فأي.

Type of attack	Description	Method and Tools
Eavesdropping	Capturing and decoding unprotected application traffic to obtain potentially sensitive information.	bsd-airtools, Ethereal, Ettercap, Kismet, commercial analyzers
Traffic Analysis	Implication of information from the observation of external traffic characteristics.	
Cracking WEP Key	Capturing data to recover a WEP key using brute force or Fluhrer-Mantin-Shamir (FMS) cryptanalysis.	Aircrack, AirSnort, chopchop, dwepcrack, WepAttack, WepDecrypt, WepLab
Evil Twin AP	Masquerading as an authorized AP by beaconing the WLAN's service set identifier (SSID) to lure users.	cqureAP, HermesAP, HostAP, OpenAP, Quetec, WifiBSD
Man-in-the-Middle Attack	Running traditional man-in-the-middle attack tools on an evil twin AP to intercept TCP sessions or SSL/SSH tunnels.	dsniff, Ettercap
Masquerading	Pretends to be an authorized user of a system in order to gain access to it.	Stealing login IDs and passwords, bypassing authentication mechanisms
Session Hijacking	Manipulating the network so the attacker's host appears to be the desired destination.	Manipulating
Honeypot Access Point	Setting its service identifier (SSID) to be the same as an access point at the local hotspot assumes the attacker as the legitimate hotspot.	Manipulating SSID

التهديدات المحتملة على الشبكات اللاسلكية: الهجمات على التوافر (Availability Attacks)

هذه الهجمات تهدف إلى عرقلة تقديم الخدمات اللاسلكية للمستخدمين الشرعيين، من خلال اما شل هذه الموارد أو بمنعهم من الوصول لموارد الشبكة المحلية اللاسلكية. وهناك العديد من الهجمات التي يستخدمها المهاجم لعرقلة توافر الشبكات اللاسلكية. وهذه الهجمات كالاتي:

Type of Attack	Description	Method and Tools
Access Point Theft	Physically removing an AP from a public space.	Five finger discount
Denial of Service	Exploiting the CSMA/CA Clear Channel Assessment (CCA) mechanism to make a channel appear busy.	An adapter that supports CW Tx mode, with a low-level utility to invoke continuous transmit
Beacon Flood	Generating thousands of counterfeit 802.11 beacons to make it hard for stations to find a legitimate AP.	FakeAP
Authenticate Flood	Sending forged Authenticates or	Airjack, File2air, Macfld, void11

	Associates from random MACs to fill a target AP's association table.	
Disassociation Attacks	Causes the target unavailable to other wireless devices by destroying the connectivity between station and the client.	Destroys the connectivity
De-authenticate Flood	Flooding station(s) with forged Deauthenticates or Disassociates to disconnecting users from an AP.	Airjack, Omerta, void11
TKIP MIC Exploit	Generating invalid TKIP data to exceed the target AP's MIC error threshold, suspending WLAN service.	File2air, wnet dinject
ARP Cache Poisoning Attack	Provides attackers with many attack vectors.	
EAP-Failure	Observing a valid 802.1X EAP exchange, and then sending the station a forged EAP-Failure message.	QACafe, File2air, libradiate
Routing Attacks	Routing information is distributed within the network.	RIP protocol
Power Saving Attacks	Transmitting a spoofed TIM or DTIM to the client while in power saving mode causes the DoS attack.	

التهديدات المحتملة على الشبكات اللاسلكية: هجمات المصادقة (Authentication Attacks)

الهدف من هذه الهجمات هو سرقة هوية عملاء خدمة الواي فاي، المعلومات الشخصية، وبيانات اعتماد تسجيل الدخول، إلخ الوصول غير المصرح به إلى موارد شبكة الاتصال.

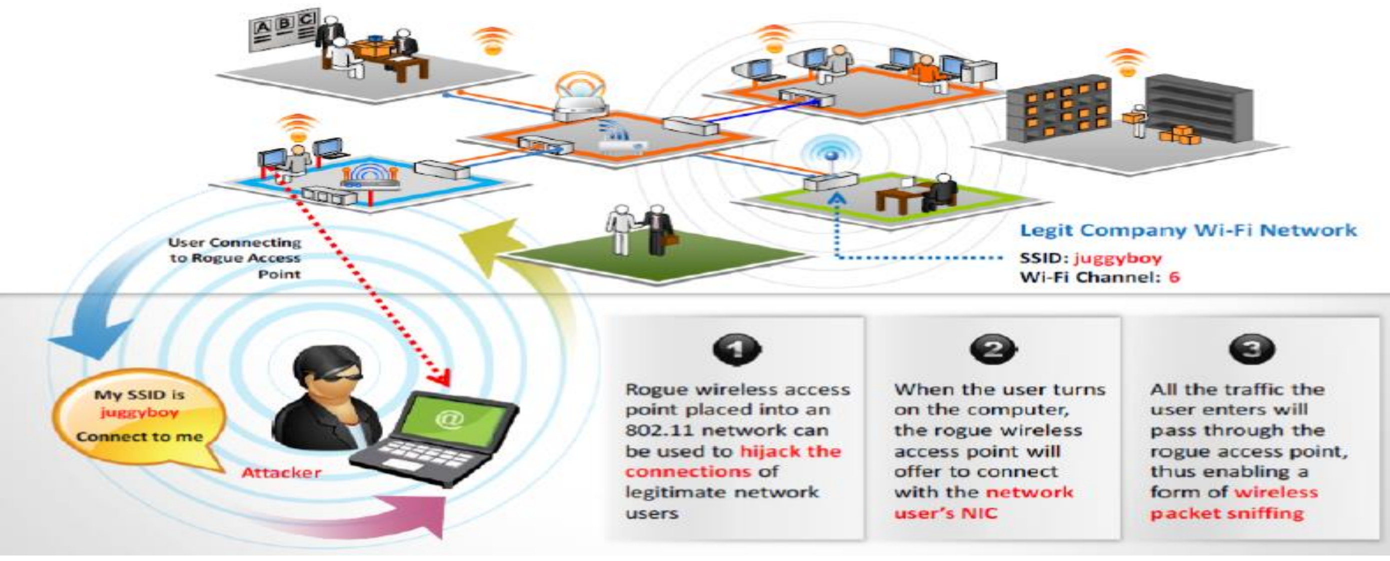
Type of Attack	Description	Method and Tools
Application Login Theft	Capturing user credentials (e.g., email address and password) from cleartext application protocols.	Ace Password Sniffer, Dsniff, PHoss, WinSniffer
PSK Cracking	Recovering a WPA PSK from captured key handshake frames using a dictionary attack tool.	coWPAtty, KisMAC, wpa_crack, wpa-psk-bf
Shared Key Guessing	Attempting 802.11 Shared Key Authentication with guessed vendor default or cracked WEP keys.	WEP cracking tools
Domain Login Cracking	Recovering user credentials (e.g., Windows login and password) by cracking NetBIOS password hashes, using a brute-force or dictionary attack tool.	John the Ripper, L0phtCrack, Cain

Identity Theft	Capturing user identities from cleartext 802.1X Identity Response packets.	Capture tools
VPN Login Cracking	Recovering user credentials (e.g., PPTP password or IPSec Preshared Secret Key) by running brute-force attacks on VPN authentication protocols.	ike_scan and ike_crack (IPsec), anger and THC-pptp-bruter (PPTP)
Password Speculation	Using a captured identity, repeatedly attempting 802.1X authentication to guess the user's password.	Password dictionary
LEAP Cracking	Recovering user credentials from captured 802.1X Lightweight EAP (LEAP) packets using a dictionary attack tool to crack the NT password hash.	Anwrap, Asleap, THC-LEAPcracker

ROGUE ACCESS POINT ATTACK

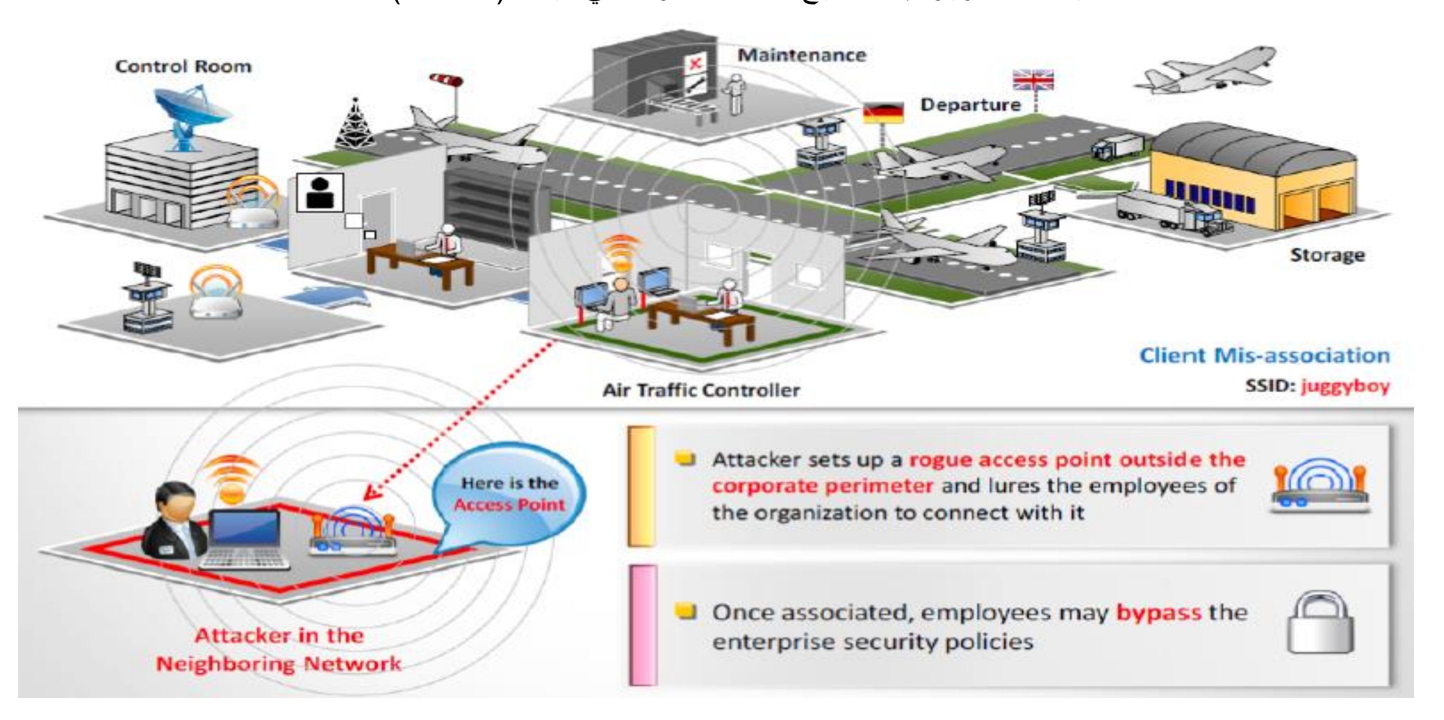
يسمح **802.11** لنقاط الوصول (**AP**) الشبكة اللاسلكية بالاتصال بـ **NIC** من خلال المصادقة مع مساعدة من **service set identifiers** (**SSIDs**). نقاط الوصول الغير مصرح به يمكنها ان تسمح لأي شخص مع جهاز **802.11** بالدخول على شبكة الشركة، ومنها يضع المهاجم على مقربه من الموارد الحرجة ذات الأهمية. مع مساعدة من أدوات **wireless sniffing tools**، يمكن تحديد ما يلي: نقاط الوصول إلى عناوين (**MAC**) أو اسم المورد، أو تكوينات الأمان. ثم يمكن ان يقوم المهاجم بإنشاء قائمة بعناوين **MAC** لنقطة الوصول المأذون بها على الشبكة المحلية، واختبار هذه القائمة مع قائمة MAC التي اوجدت من خلال **sniffing**.

ثم يمكن للمهاجم إنشاء **rogue access point** (نقاط الوصول الاحتيالية) الخاص به ووضعه بالقرب من شبكة الشركات المستهدفة. يمكن استخدام نقطة الوصول هذه التي تم وضعها في شبكة **802.11** لخطف اتصالات مستخدمي الشبكة المشروعة. عندما يقوم المستخدم بتشغيل الكمبيوتر، سوف يتوفر نقطة وصول لاسلكية مزيفه (**rogue access point**) للاتصال مع **NIC** لمستخدم الشبكة. المهاجم يغري المستخدم للاتصال بنقطة الوصول هذه بإرسال **SSID**. إذا كان المستخدم يتصل بنقطة الوصول الاحتيالية باعتباره جهاز **AP** مشروع، فان كل حركة المرور التي قام المستخدم بإدخالها سيمر عبر **rogue access point**، وبالتالي تمكين نموذج **wireless packet sniffing**. الحزم التي تم التنصت عليها (**sniffed packet**) قد تحتوي على اسم المستخدم وكلمات المرور.



CLIENT MIS-ASSOCIATION

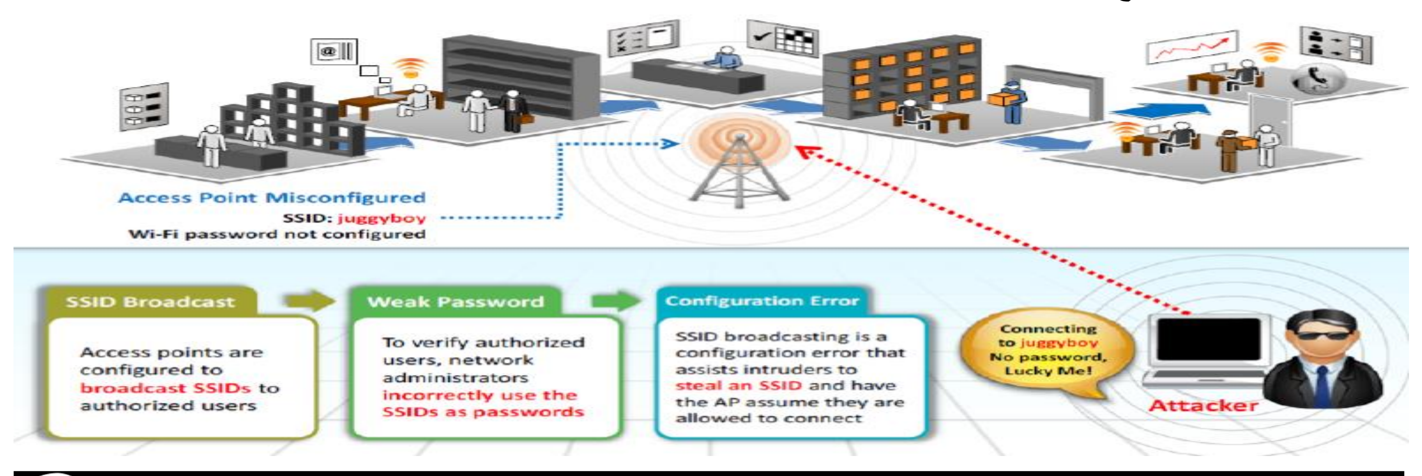
المهاجم يقوم بإعداد نقطة وصول احتياليه خارج محيط الشركات ومن ثم يغري العاملين في المنظمة للتواصل معها. وهذا من الممكن ان يستخدم كقناة لتجاوز نهج أمان المؤسسة. عندما يتصل العميل لاسلكيا بنقطة الوصول الاحتيالية، فان المهاجم يمكنه سرقة المعلومات الحساسة مثل أسماء المستخدمين وكلمات المرور بإطلاق نوع من هجمات رجل في الوسط (**MITM**).



CLIENT MIS-ASSOCIATION

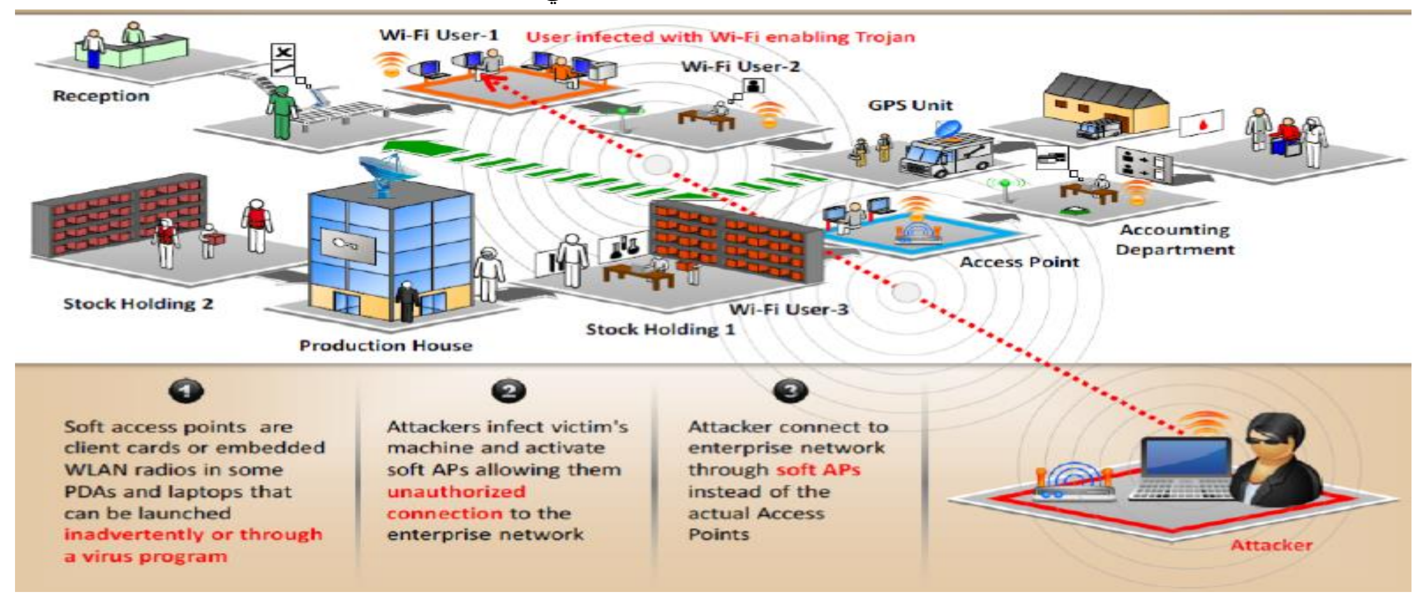
معظم المنظمات تنفق مقدار كبير من الوقت في تحديد وتنفيذ سياسات أمن الواي فاي، ولكن قد يمكن لعميل شبكة الاتصال اللاسلكية تغيير الإعدادات الأمنية لنقطة الوصول (**AP**)عن غير قصد؛ وهذا بدوره قد يؤدي إلى تكوينات الخاطئة الى نقاط الوصول. يمكن أن يعرض **AP misconfigured** الشبكة الأمنه جيدا للهجمات. المهاجمين يمكنهم بسهولة الاتصال بالشبكة الأمنه من خلال نقاط الوصول **misconfigured**. وفيما يلي العناصر التي تلعب دوراً هاما في هذا النوع من الهجوم:

- **SSID Broadcast**: يتم تكوين نقاط الوصول لبث **SSID** للمستخدمين المصرح بهم.
- **كلمة مرور ضعيفة (Weak Password):** للتحقق من المستخدمين المخولين لهم، فان مسؤولي شبكة الاتصال يستخدمون بشكل غير صحيح **SSID** ككلمات المرور.
- **خطأ في التكوين (configuration error):** بث **SSID** هو خطأ في تكوين يساعد الدخلاء في سرقة **SSID**، ولديه افتراض لنقط الوصول يسمح له بالاتصال.



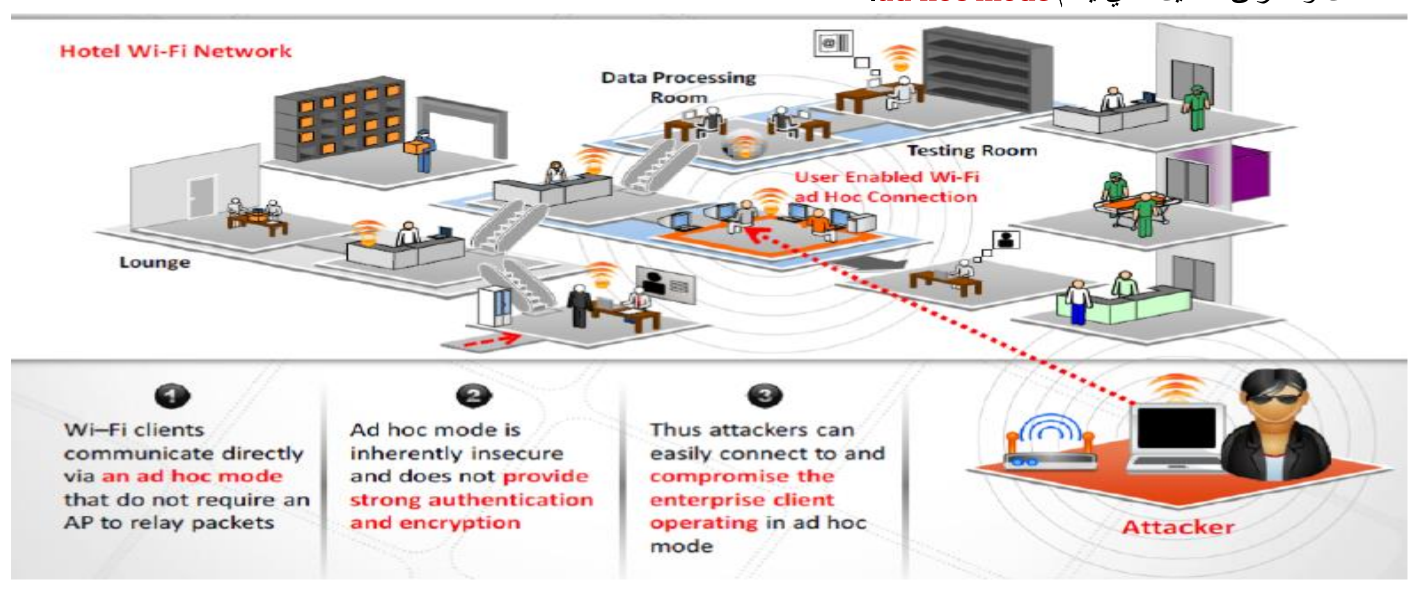
UNAUTHORIZED ASSOCIATION

الارتباط الغير مصرح به يعتبر تهديدا رئيسيا لشبكة الاتصال اللاسلكية. وهذا قد يكون واحداً من نوعين: **accidental association** أو **malicious association**. ويتم إنجاز **malicious association** مع مساعدة من **soft APs**. المهاجمون يستخدمون **soft APs** للحصول على حق الوصول إلى شبكة الاتصال اللاسلكية للهدف. برمجيات نقاط الوصول (**software access point**) هي بطاقات العميل أو **WLAN radios** مضمنه في بعض أجهزة **PDAs** وأجهزة الكمبيوتر المحمولة التي يمكن إطلاقها عن غير قصد أو عن طريق برنامج فيروسات. المهاجمين يصيبون جهاز الضحية ومن ثم تنشيط **soft APs**، مما يتيح لهم الاتصال بشبكة المؤسسة دون إذن. المهاجمين يتصلون بشبكة المؤسسة من خلال **soft APs** بدلاً من نقاط الوصول الفعلي.



AD HOC CONNECTION ATTACK

عملاء خدمة الواي فاي يتواصلون مباشرة عن طريق **ad hoc mode** التي لا تتطلب من نقاط الوصول **relay packets**. الشبكات التي ترتبط في الوضع **ad hoc mode** تتبادل المعلومات عبر العملاء. لمشاركة محتوى الصوت/الفيديو مع الآخرين، فان معظم مستخدمي الواي فاي يستخدمون شبكات **ad hoc**. أحياناً يتم إجبار الشبكات لتمكين وضع **ad hoc mode** من خلال الموارد التي يمكن الوصول إليها فقط في الوضع **ad hoc**، ولكن هذا الوضع هو أصلاً غير أمن ولا يوفر قوي المصادقة والتشفير هكذا، والمهاجمين يمكنهم بسهولة الاتصال واختراق العميل الذي يقدم **ad hoc mode**.



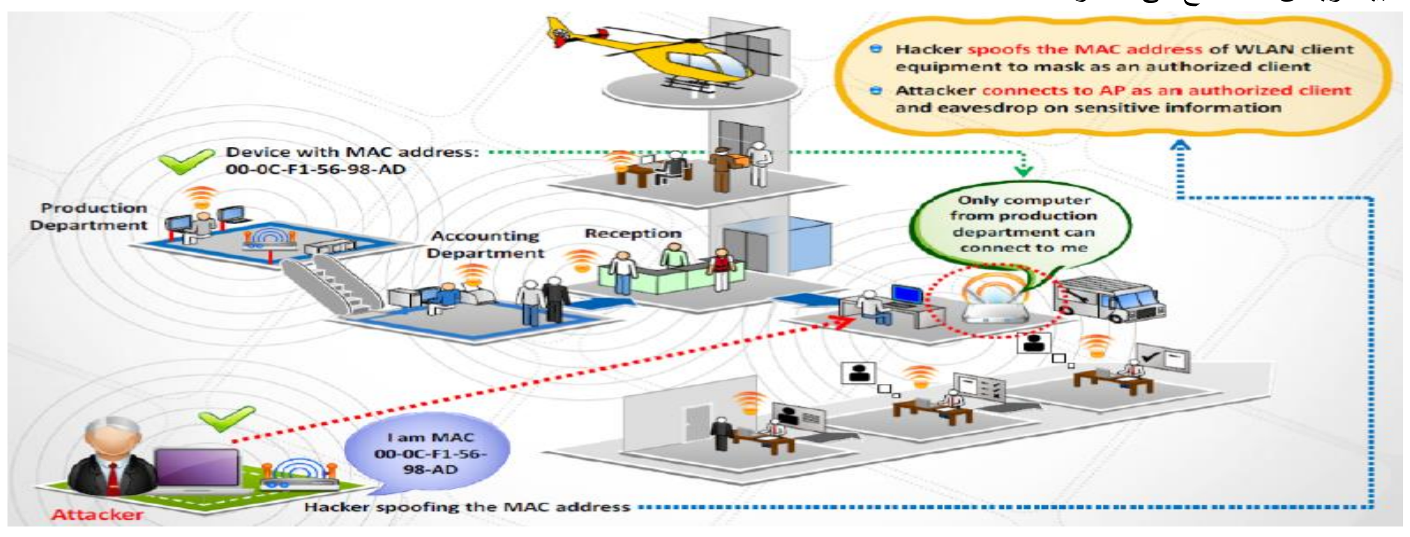
HONEYSPOT ACCESS POINT ATTACK

يمكن للمستخدمين الاتصال بأي شبكة متوفرة في حالة شبكات **WLANS** المتعددة التي تتعايش في نفس المساحة. هذا النوع من الشبكات اللاسلكية المتعددة أكثر قابلة للاستغلال بسبب الهجمات. المهاجمين يمكنهم إعداد شبكة لاسلكية غير مصرح بها عن طريق تشغيل نقطة الوصول في منطقة شبكات **WLANS** المتعددة ويمكن أن يسمح لمستخدمين الشبكات المأذون بها الحصول على اتصال به. وتسمى **APs** هذه التي شنت من قبل المهاجم **honeypot**. هذه **APs** تنقل إشارة **beacon** أقوى. بطاقات الشبكة اللاسلكية عادة تبحث عن إشارات قوية للوصول. ومن ثم المستخدمين المخول لهم يتصلون بهذه **malicious honeypot AP**؛ وهذا يخلق ثغره امنيه ويرسل المعلومات الحساسة للمستخدم مثل الهوية واسم المستخدم وكلمة المرور للمهاجم.



AP MAC SPOOFING

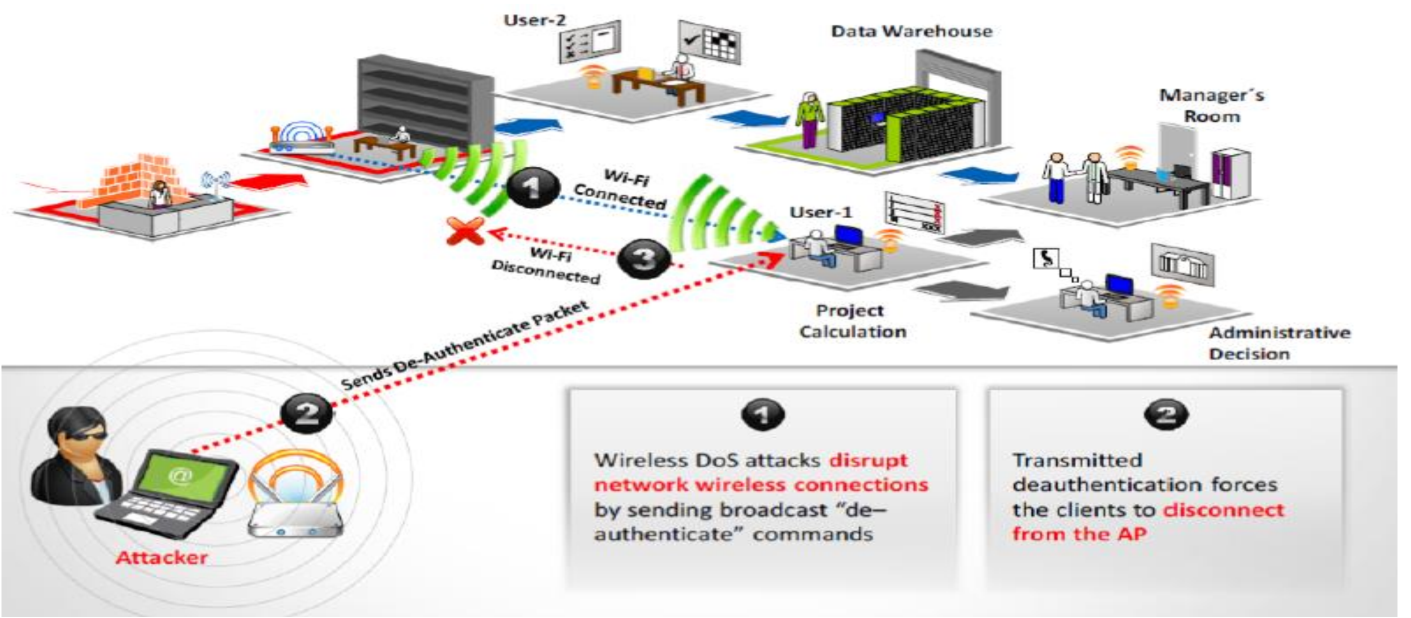
في شبكات **LAN** اللاسلكية، نقاط الوصول تقوم بإرسال (**beacons**) **probe responses** لتعلن عن وجودها في الهواء. **Probe responses** تحتوي على معلومات حول هويته (عنوان **MAC**) وهوية الشبكة التي تدعمه (**SSID**). العملاء في محيط الشبكة يقومون بالاتصال بهذه الشبكة عن طريق **beacons** استناداً إلى عنوان **MAC** ومعرف **SSID** الذي يحتويه. العديد من أدوات البرمجيات، ومعظم نقاط الوصول تسمح بتعيين القيم المعرفة من قبل المستخدم لعناوين **MAC** و **SSID** لأجهزة نقاط الوصول. المهاجمين يقومون بانتحال عنوان **MAC** لنقاط الوصول من خلال برمجة **AP** للإعلان بالضبط نفس معلومات الهوية كما في **AP** الضحية. المهاجمين يقومون بانتحال عنوان **MAC** لمعدات العميل **LAN** اللاسلكية للتنكر كعميل مشروع والاتصال بـ **AP**. بمجرد قيام المهاجم بالاتصال بـ **AP** كعميل مشروع له، فأنه يصبح يملك حق الوصول الكامل إلى الشبكة كأنه عميل مشروع والمهاجم يمكنه استخدام هذا الاتصال من أجل أغراض خبيثة ويمكن الاستماع الى المعلومات الحساسة.



DENIAL-OF-SERVICE ATTACK

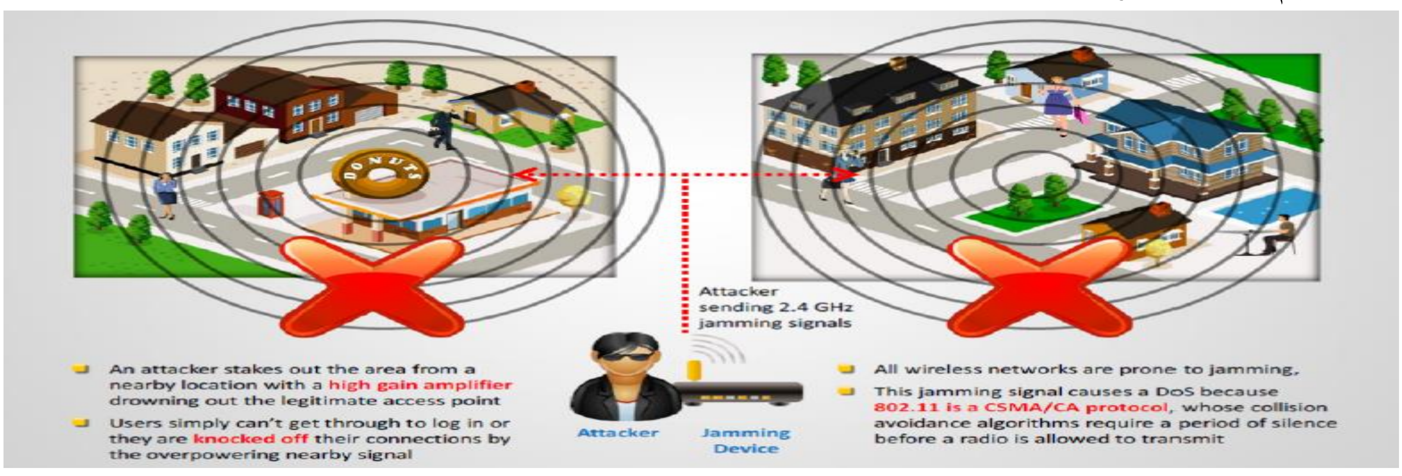
الشبكات اللاسلكية عرضه لهجمات الحرمان من الخدمة (**DoS**). عادة ما تكون هذه الشبكات تعمل في نطاقات غير مرخصة ونقل البيانات تكون في شكل إشارات الراديو. مصممين بروتوكول **MAC** يهدفون إلى الحفاظ على أنها بسيطة، ولكن لها مجموعتها الخاصة من العيوب التي هي أكثر جاذبية لهجمات **DoS**. عادة ما تحمل شبكات **WLAN** التطبيقات ذات المهام الحرجة مثل **VoIP**، **Database access**، **project data files**، والوصول إلى شبكة الإنترنت. ومن السهل تعطيل هذه التطبيقات الهامة في شبكات **WLAN** بهجوم **DoS**. هذا عادة ما يسبب فقدان الإنتاجية أو الشبكة تقف عن العمل. أمثلة على هجمات **MAC DoS**: **de-authentication flood attack**، **virtual jamming**، و **association flood attacks**.

هجمات دوس اللاسلكية تعطل اتصالات شبكة الاتصال اللاسلكية بإرسال بث **de-authenticate commands**. بث **deauthenticate** يجبر العملاء على قطع الاتصال بنقاط الوصول (**AP**).



Jamming Signal Attack

هجمات التشويش "**Spectrum jamming attacks**" هي عادة تقوم بغلق جميع الاتصالات بالكامل. يمكن إجراء هذا النوع من الهجوم بمساعدة الأجهزة المتخصصة. المهاجم يهدم منطقه معينه من أقرب مكان مع **high gain amplifier** من خلال التخلص من نقاط الوصول المشروعة. المستخدمين ببساطة لا يمكن الحصول على طريق لتسجيل الدخول أو يطردوا من اتصالهم بالشبكة من خلال سحق الاشارات القريبة. جميع الشبكات اللاسلكية عرضه للتشويش. الإشارات التي تم إنشاؤها بواسطة أجهزة التشويش، على ما يبدو، تنقل اشارات **802.11** للأجهزة الموجودة على الشبكة اللاسلكية، مما يسبب لهم الاحتفاظ بها حتى تهدأ الإشارة مما ينتج الحرمان من الخدمة. هذه الهجمات يتم ملاحظتها بسهولة نسبيا.



- **Wi-Fi Jamming Devices**

اجهز تشويش الواي فاي هي نوع من الهجوم على الشبكات اللاسلكية. يمكن أن يتم ذلك باستخدام بعض الأجهزة. استخدام الأجهزة التي يستخدمها المهاجم للتشويش اللاسلكي تستخدم نفس نطاق التردد لشبكة اتصال موثوق بها الذي يريد المهاجم شن الهجوم عليها. أجهزة التشويش اللاسلكي توليد الإشارات مع نفس التردد لإشارات الشبكة اللاسلكية الموثوق بها. وهذا يؤدي الى التدخل مع الإشارة المشروعة مما يعطل مؤقتا خدمة شبكة الاتصال. وفيما يلي عدد قليل من أجهزة التشويش اللاسلكي:



15.4 منهجية قرصنة الشبكات اللاسلكية "Wireless Hacking Methodology"

الشبكات اللاسلكية عرضه للعديد من الثغرات الأمنية. حتى من خلال آليات الأمن السليم التي يتم توظيفها من قبل المنظمات، قد لا يزال ضعيفا. وهذا يرجع إلى أن آليات الأمن أنفسها قد تحتوي على ثغرات. المهاجمين يمكنهم قرصنة الشبكة اللاسلكية باستغلال تلك الثغرات أو العيوب في آليات الأمن. من اجل اكتمال نطاق اختبار الاختراق، يجب على مختبر الاختراق اتباع منهجية قرصنة الشبكة اللاسلكية.

WI-FI Discovery

هدف منهجية قرصنة الشبكة اللاسلكية هو اختراق شبكة الواي فاي بغية الوصول غير المصرح به إلى موارد شبكة الاتصال. المهاجمين عادة ما يتبعوا منهجية القرصنة لضمان عدم تفويت حتى نقطة دخول واحدة لاقتحام الشبكة المستهدفة. اكتشاف الشبكة اللاسلكية أو الجهاز هو الإجراء الأول الذي ينبغي أدائه من قبل المهاجم. يمكنك تنفيذ اكتشاف شبكة الواي فاي مع مساعدة من الأدوات مثل **insider**، **NetSurveyor**، **NetStumbler**، **Vistumbler**، **WirelessMon**، إلخ.

عملية الاستطلاع عن الشبكات اللاسلكية (Footprint the Wireless Network)

مهاجمة الشبكة اللاسلكية يبدأ مع اكتشاف واستطلاع "**Footprinting**" شبكة الاتصال اللاسلكية. **Footprinting** ينطوي على تحديد وتحليل (أو فهم) شبكة الاتصال. **Footprinting** الشبكة اللاسلكية يمكن أن يتم بطريقتين.

من أجل أداء **Footprinting** للشبكة اللاسلكية فيجب عليك أولا تحديد **BSS** التي يتم توفيرها من قبل نقطة الوصول (**AP**). يمكن تحديد **BSS** أو **IBSS** مع مساعدة **SSID**. المهاجم يمكن استخدام **SSID** هذا لإنشاء رابطة مع **AP**.

طرق أداء الـ Footprinting:

- **Passive method:**

يمكن للمهاجمين استخدام الطريقة السلبية للكشف عن وجود **AP** من خلال التنصت على الحزم امن موجات **airwaves**، التي يمكن أن تكشف عن **AP**، **SSID**، وأجهزة المهاجم اللاسلكية التي تعمل حاليا.

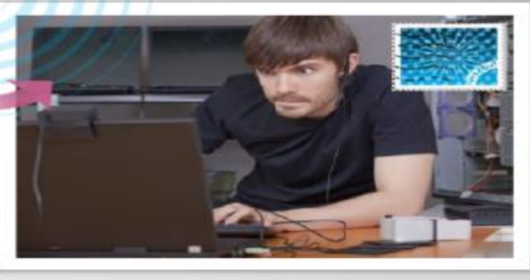
- **Active method:**

في هذا الأسلوب، يرسل الجهاز اللاسلكي الخاص بالمهاجم طلب تحقيق (**probe request**) مع **SSID** لترى إذا كان **AP** أم لا. إذا لم يكن لديه **SSID** الجهاز اللاسلكي في البداية، فإنه يمكن إرسال طلب التحقيق (**probe request**) مع **SSID** فارغ. في حالة طلب التحقيق مع **SSID** فارغ، فان معظم **AP** تستجيب مع **SSID** الخاصة به في حزمة استجابة (**probe response packet**). ونتيجة لذلك، فان استخدام **SSIDs** فارغة مفيد في معرفة **SSID** الخاص بـ **AP**. هنا يعرف المهاجم **BSS** الصحيح لإجراء اقتران معه. يمكن اعداد AP لتجاهل طلب التحقيق (**probe request**) مع **SSID** فارغ.

المهاجمين يقومون بفحص الشبكات اللاسلكية (Attackers Scanning for Wi-Fi Networks)

يمكن للمهاجمين فحص شبكات اللاسلكية مع مساعدة من أدوات فحص الشبكة اللاسلكية مثل **NetSurveyor**، **Retina WI-FI scanner**، إلخ. يمكن العثور (**Service set identifier (SSID**) في **beacon** وطلبات التحقيق والردود (**probe requests and responses**)، وطلبات الربط وإعادة الربط (**association and reassociation requests**). يمكن للمهاجم الحصول على **SSID** الشبكة عن طريق الفحص **passive scanning**. إذا فشل المهاجم في الحصول على **SSID** عن طريق الفحص **passive scanning**، فأنه يمكن تحديده من خلال **Active scanning**. وبمجرد نجاح المهاجم في تحديد **SSID**، فأنه يمكن الاتصال بشبكة الاتصال اللاسلكية وشن الهجمات المختلفة. فحص الشبكة اللاسلكية يسمح بالتنصت بضبط مختلف قنوات الراديو للأجهزة.






إيجاد شبكة الواي فاي

المهمة الأولى التي يمكن أن يمر بها المهاجم عندما يبحث عن أهداف الواي فأي هو التحقق من الشبكات المحتملة التي في النطاق للعثور على أفضل واحد للهجوم. يمكن العثور على شبكات الواي فاي من خلال تمكين كارت الواي فاي في الجهاز المحمول (**laptop**). يجب على **laptop** ان يحمل أداة لاكتشاف الشبكات اللاسلكية مثبتة عليه. باستخدام أداة الاكتشاف، فان المهاجم يمكنه أن يرسم الشبكات اللاسلكية النشطة. لاكتشاف شبكات الواي فاي، يحتاج المهاجم:

- Laptop with Wi-Fi card (جهاز كمبيوتر محمول مع كارت واي فاي)
- External Wi-Fi antenna (هوائي واي فاي خارجي)
- Network discovery programs (برنامج لاكتشاف الشبكة).

العديد من أدوات اكتشاف شبكة الواي فاي تكون متاحه على شبكة الإنترنت والتي تعطى المزيد من المعلومات حول الشبكات اللاسلكية في المنطقة المجاورة. وتشمل أمثلة من هذه الأدوات التي يمكن استخدامها للعثور على شبكات الواي فاي **inSSIDer**، **NetSurveyor**، **NetStumbler**، **Vistumbler**، إلخ.

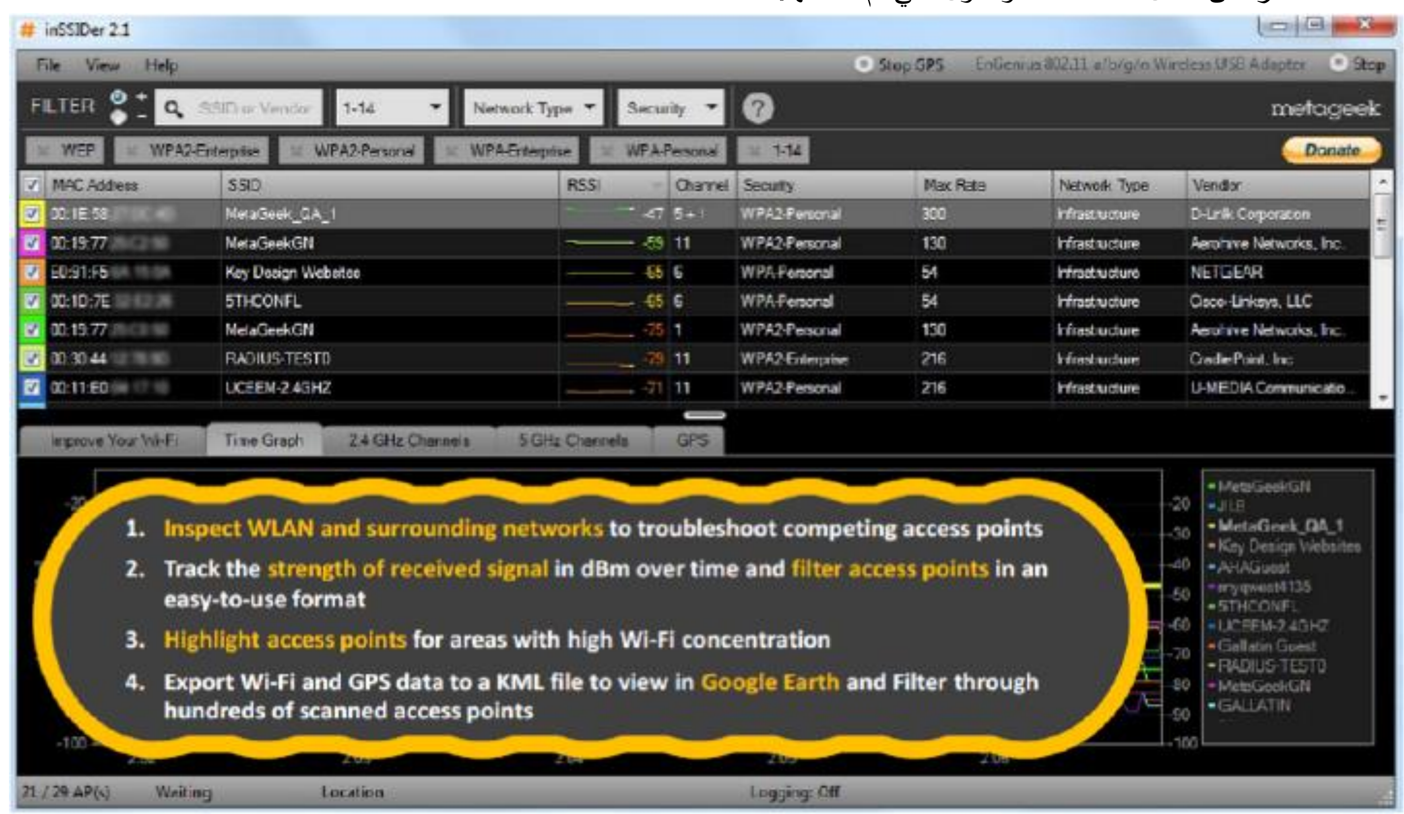
Wi-Fi Discovery Tool: inSSIDer

المصدر: http://www.metageek.com

InSSIDer هي برنامج لفحص الواي فاي. يعمل مع ويندوز فيستا/7 وأجهزة الكمبيوتر 64 بت. أنه يستخدم **Native Wi-Fi API** وبطاقة الشبكة اللاسلكية الحالية، وفرز النتائج حسب عنوان **MAC**، **SSID**، **channel**، **RSSI**، و**Time Last Screen**.

SSID يفعل الاتي:

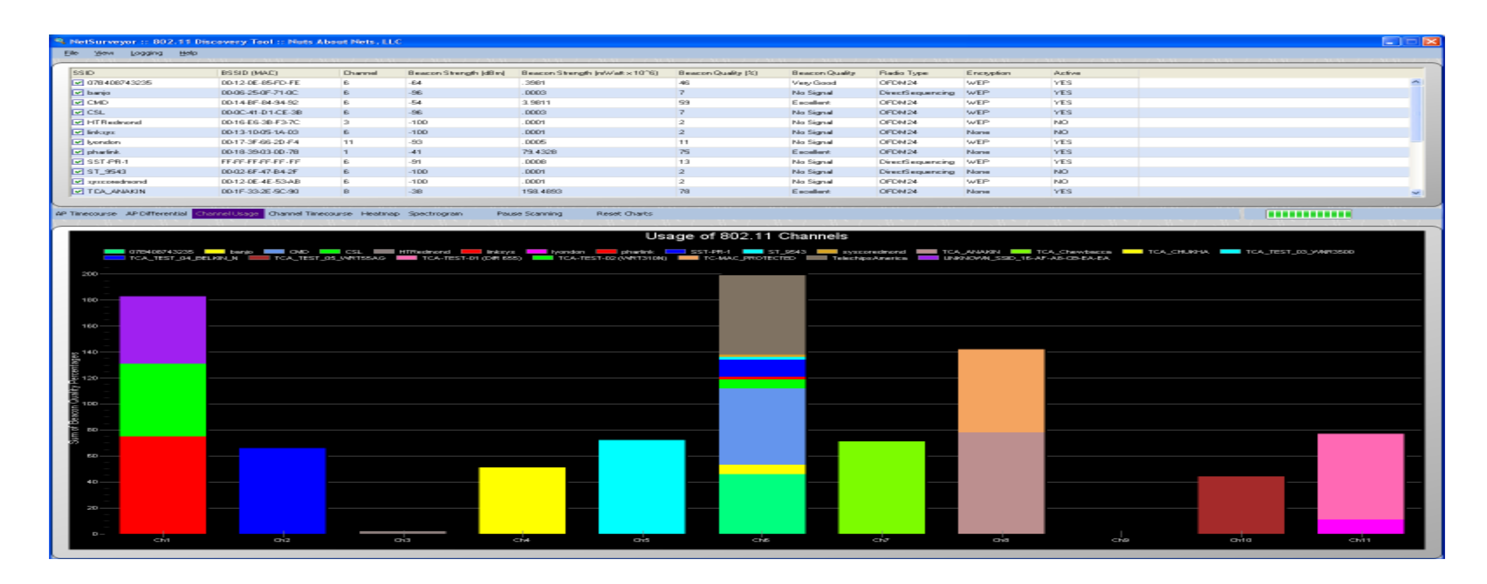
- فحص الشبكات اللاسلكية **WLAN** والشبكات المحيطة بها لمعالجة مشاكل نقاط الوصول المتنافسة.
- يتتبع قوة إشارة الاستقبال في **dBm over time**.
- فلترة نقاط الوصول في صيغة سهولة الاستخدام.
- تسليط الضوء على نقاط الوصول في المناطق ذات التركيز الاعلى للواي فاي.
- تصدير بيانات الواي فاي، ونظام GPS الى ملف **KML** لعرضه بواسطة **Google Earth**.
- الفلترة من خلال مئات نقاط الوصول التي تم فحصها.



Wi-Fi Discovery Tool: NetSurveyor

المصدر: http://nutsaboutnets.com/netsurveyor-wifi-scanner

نيتسورفييور هو أداة اكتشاف شبكة 802.11 (واي فاي) والذي يقوم بجمع معلومات حول مكان أقرب نقاط الوصول اللاسلكية في الوقت الحقيقي، ويعرضه بطرق مفيدة. يتم عرض البيانات باستخدام مجموعة متنوعة من الوجهات الفحص المختلفة والرسوم البيانية. يمكن تسجيل البيانات لفترات طويلة والعودة اليها في تاريخ/وقت لاحق. أيضا، يمكن إنشاء التقارير في تنسيق **PDF**.

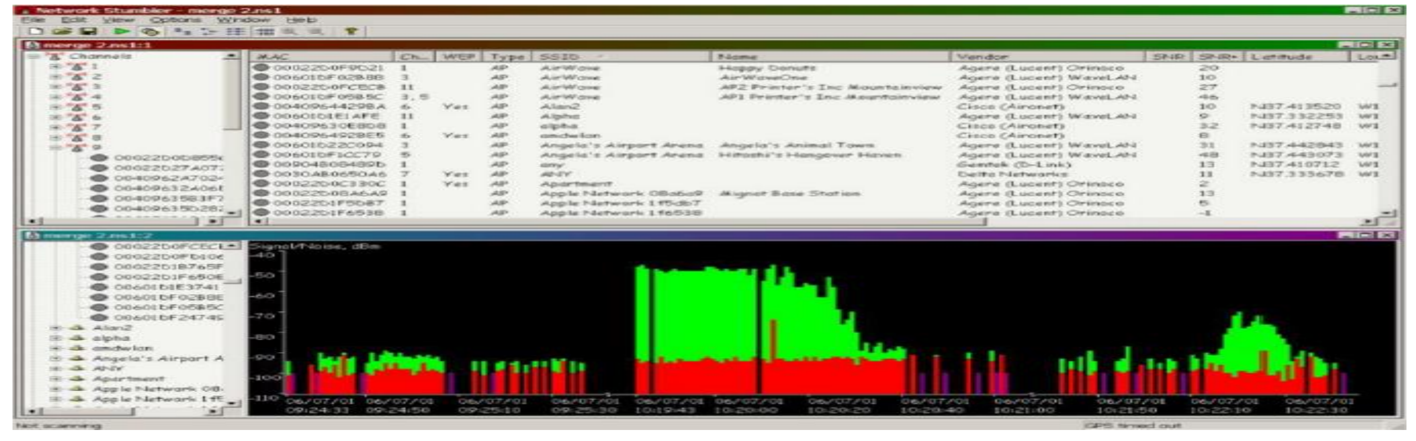


Wi-Fi Discovery Tool: NetStumbler

المصدر: http://www.netstumbler.com
NetStumbler هو أداة للتنصت على الإشارات اللاسلكية وإعلام المستخدمين إذا كان تكوين الشبكة اللاسلكية بشكل صحيح. ولكن قبل تحميله، فان المستخدمين بحاجة أولا إلى التحقق من ان بطاقاتهم اللاسلكية تكون متوافقة مع **NetStumbler**. والخطوة التالية هو تعطيل الخدمة **automatic configuration service of the said device**. على سبيل المثال، مستخدمي أجهزة ويندوز، يجب عليهم إيقاف الخدمة **Windows Wireless Zero Configuration (WLAN AutoConfig)**، التي يمكن أن تكون موجودة في **Control Panel** ثم **Administrative tools** ثم **services**.
NetStumbler يضم العديد من الأعمدة التي توفر معلومات مفيدة في الكشف عن الإشارات. عمود التحكم بالوصول إلى الوسائط أو الماك يعكس قوة إشارة كما هو مبين باللون من بين النقاط التي تمثل كل إدخال. رمز القفل داخل النقطة يتوقع ان نقاط الوصول مشفره. عمود **SSID** يحدد موقع شبكة الاتصال التي تأتى الحزم اللاسلكية منه. يظهر العنوان **Chan** (**channel**) أي قناة من نقاط وصول الشبكة تقوم ببث الإشارة، وإلى جانب ذلك عمود لتحديد سرعة القناة، والتي يتم التعبير عنها بالميجابايات في الثانية. العنوان **vendor** يكشف عن اسم الشركات المصنعة للأجهزة مثل **Linksys**، **Netgear**، **D-link**، و**2Wire** بينما العمود **Signal-to-Noise Ratio** يشير إلى جوده إشارة الواي فاي.

الاستخدام الشائع:

- Wardriving
- Verifying network configurations
- Finding locations with poor coverage in one’s WLAN
- Detecting causes of wireless interference
- Detecting unauthorized ("rogue") access points
- Aiming directional antennas for long-haul WLAN links



Wi-Fi Discovery Tool: Vistumbler

المصدر: http://www.vistumbler.net

Vistumbler هو برنامج لفحص الشبكة اللاسلكية. فإنه يقوم بتعقب إجمالي نقاط الوصول **w/gps**، الرسوم البيانية للإشارة، والإحصاءات، وأكثر.

السمات:

- يدعم ويندوز فيستا وويندوز 7.
- إيجاد نقاط الوصول اللاسلكية -يستخدم أوامر ويندوز فيستا "**netsh wlan show networks mode=bssid**" للحصول على المعلومات اللاسلكية.
- يدعم **GPS**.
- تصدير/استيراد نقاط الوصول من **Vistumbler TXT/VSl/VSZ** او **Netstumbler TXT/Text NS1**.
- تصدير مواقع **GPS** لنقاط الوصول الى ملف **Google earth** او (**GPS eXchange format**) **GPX**.
- التتبع من خلال **Google earth**: تلقائياً يظهر نقاط الوصول في **Google earth**.
- يذكرك بقوة الإشارة باستخدام ملفات الصوت أو واجه الويندوز الصوتية أو **MIDI**.

Vistumbler v10.11 - By Andrew Calcutt - 2011/11/11 - (2011-11-21 23-57-00.mdb)

File Edit Options View Settings Interface Extra WifiDB Help *Support Vistumbler*

Stop | Use GPS | Graph1 | Graph2

Active APs: 30 / 53
Actual loop time: 1012 ms

Latitude: N 0000.0000
Longitude: E 0000.0000

Authentication
Channel
Encryption
Network Type
SSID

#	Active	SSID	Signal	High Signal	Authentication	Encryption
34	Dead	TP-LINK	0%	88% (-38...	WPA2-PSK	AES
33	Dead	linksys22F	0%	30% (-78...	WPA-PSK	AES
32	Dead	KUO_BELKIN	0%	26% (-81...	Open	WEP
31	Dead	ling-Home	0%	32% (-77...	WPA2-PSK	AES
30	Active	JackyPO	26% (-...	88% (-38...	Open	WEP
29	Active		38% (-...	60% (-58...	WPA-PSK	TKIP
28	Active	LIANE-PC_Net...	100% ...	100% (-30...	WPA2-PSK	AES
27	Dead	Rajpriya	0%	16% (-88...	WPA2-PSK	AES
26	Active	BUFFALO	38% (-...	88% (-38...	Open	WEP
25	Dead	Kiang	0%	88% (-38...	Open	Unencrypted
24	Active	HSPAWirelessG...	36% (-...	88% (-38...	WPA-PSK	TKIP
23	Active	Bonjour	38% (-...	88% (-38...	WPA2-PSK	AES
22	Active	HOME	34% (-...	88% (-38...	WPA2-PSK	AES
21	Active	Lai's home	28% (-...	30% (-78...	Open	WEP
20	Active	superlink	88% (-...	88% (-38...	WPA-PSK	TKIP
19	Active	linksys	34% (-...	88% (-38...	WPA2-PSK	AES
18	Dead	yee_family	0%	88% (-38...	WPA2-PSK	AES
17	Active	EWHOME	36% (-...	36% (-74...	WPA2-PSK	AES
16	Active	Philip	26% (-...	88% (-38...	WPA-PSK	TKIP
15	Active	dlink	10% (-...	18% (-86...	Open	Unencrypted
14	Active	Ng's Family	46% (-...	88% (-38...	WPA2-PSK	AES
13	Active	speed-1	74% (-...	88% (-38...	WPA2-PSK	AES

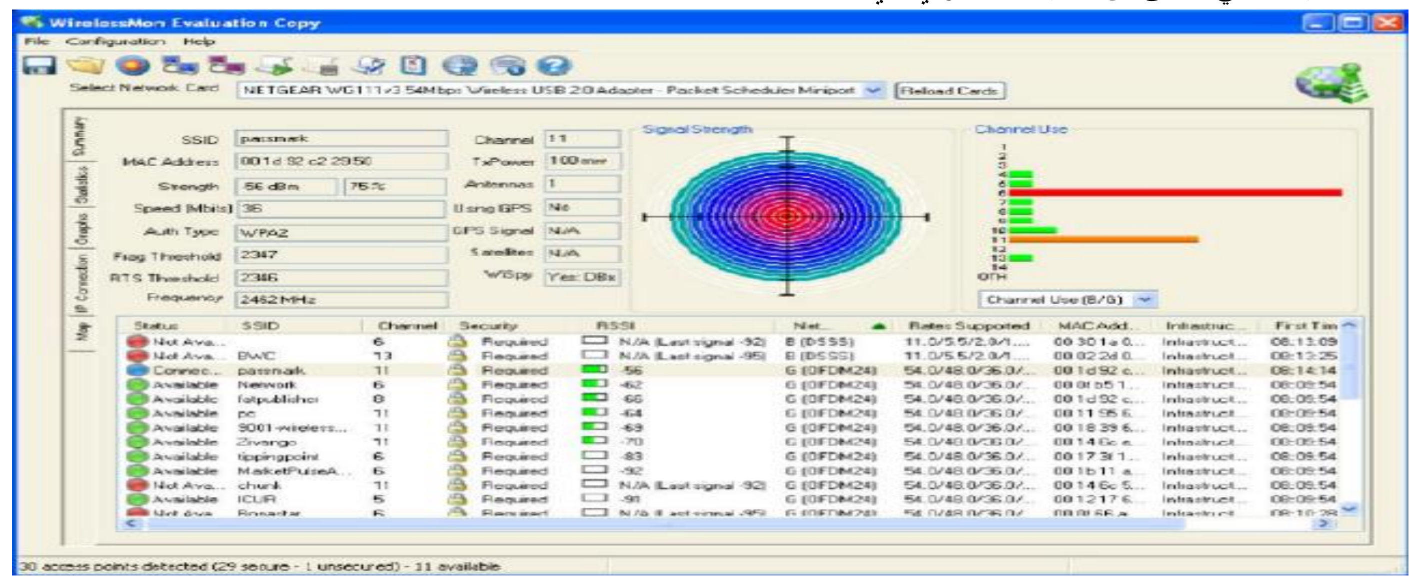
Wi-Fi Discovery Tool: WirelessMon

المصدر: http://www.passmark.com

WirelessMon هو أداة برمجيات تسمح للمستخدمين برصد حالة محول الواي فاي اللاسلكية، وجمع معلومات حول مكان اقرب نقاط الوصول اللاسلكية والنقاط الساخنة في الوقت الحقيقي. **WirelessMon** يمكنه تسجيل المعلومات التي يجمعها في ملف، بينما يوفر أيضا رسوم بيانية شاملة عن مستوى الإشارة وإحصاءات **IP** و**802.11 Wi=Fi** في الوقت الحقيقي.

بعض من مميزات **WirelessMon** تشمل:

- التحقق من ان اعداد شبكة 802.11 بشكل صحيح.
- اختبار برامج تشغيل جهاز الواي فاي والأجهزة تعمل بشكل صحيح.
- فحص مستويات الإشارة من الشبكة اللاسلكية المحلية والشبكات المجاورة.
- المساعدة في العثور على واجهة شبكة الاتصال الخاصة بك.
- فحص النقاط الساخنة في منطقتك المحلية (**wardriving**).
- تدعيم **GPS** وإنشاء خرائط لقوة الإشارة.
- تسجيل ورسم خرائط قوة الإشارة التي يمكن أن يؤديها مع أو بدون **GPS**.
- تحديد موقع الهوائي اللاسلكي الخاص بك بشكل صحيح.
- التحقق من إعدادات الأمان لنقطة الوصول المحلي.
- قياس سرعة الشبكة وعرض معدلات البيانات المتاحة.
- يساعد في التحقق من تغطية شبكة الواي فاي.



Mobile-based Wi-Fi Discovery Tool

- **WiFiFoFum - WiFi Scanner**

المصدر: http://www.dynamicallyloaded.com

WiFiFoFum هو فاحص الشبكات اللاسلكية من خلال الموبايل والتي تسمح لك لفحص شبكات **Wi-fi 802.11**. وهذا يوفر لك معلومات حول كل شبكة يتم الكشف عنها ويعطي معلومات مفصلة حول شبكات **SSID**، ماك، **RSSI** (قوة الإشارة)، **channel**، **AP mode**، الوضع الأمني، ومعدلات الإرسال المتوفرة. فإنه يمكن فحص الشبكات المحيطة بها، واكتشاف الوصول إلى الإنترنت، ويعطي معلومات الاعداد **AP** الشامل.



▪ Network Signal Info

المصدر: http://www.kaibits-software.com

Network Signal Info يوفر معلومات مفصلة عن شبكة الاتصال المستخدمة حاليا، بغض النظر عن ما إذا كنت تستخدم واي فاي أو اتصال الهاتف الخلوي.



▪ WiFi Manager

المصدر: http://kmansoft.com

WiFi Manager هي البرمجيات التي تسمح لك للحصول على شرح كامل لحالة الاتصال اللاسلكي التي يتم استخدامها مع **screenshot widget**. يمكنك الحصول على معلومات حول عند أنه كان تبديل تشغيل/إيقاف عملية الاتصال، ومؤشرا على مستوى إشارة الشبكة، و**SSID** للشبكة الحالية.



▪ OpenSignalMaps

المصدر: http://opensignal.com

هذا الموقع يقدم لك مع التصور والبيانات المستمدة من الدراسة بجانب الإشارات الدقيقة لمقدمي الخدمات في مجال معين مع خرائط التغطية الخلوية.



Wi-Fi Discovery Tools

أدوات اكتشاف الواي فاي يمكن اكتشاف الشبكات (**BSS/IBSS**) واكتشاف بث **ESSID** أو شبكات الغير مبثه وقدراتها على **WEP** والشركة المصنعة. هذه الأدوات تمكن بطاقة الواي فاي في البحث عن الاتصالات اللاسلكية المؤمنة والغير مؤمنه حيث أنت. يتم سرد عدد قليل من أدوات اكتشاف الواي فاي على النحو التالي:

WiFi Hopper available at http://www.wifihopper.com
Wavestumbler available at http://www.cqure.net
iStumbler available at http://www.istumbler.net
WiFinder available at http://www.pgmsoft.com
Meraki WiFi Stumbler available at http://meraki.com
Wellenreiter available at http://wellenreiter.sourceforge.net
AirCheck Wi-Fi Tester available at http://www.flukenetworks.com
AirRadar 2 available at http://www.koingosw.com
Xirrus Wi-Fi Inspector available at http://www.xirrus.com
Wifi Analyzer available at http://a.farproc.com

GPS MAPPING

هدف منهجية قرصنة الشبكة اللاسلكية هي اختراق شبكة الواي فاي بغية الوصول الغير مصرح به إلى موارد شبكة الاتصال. لتحقيق هذا الهدف، فسوف تحتاج أولاً الى اكتشاف شبكات الواي فاي ومن ثم القيام بـ **GPS mapping** للشبكات.
نظام تحديد المواقع (GPS) تم انشائه وتمويله والسيطرة عليه من خلال وزارة الدفاع الأمريكية (**DOD**). قد صممت خصيصا للجيش الأمريكي، ولكن أصبح العديد من المستخدمين المدنيين يستخدمون تحديد المواقع في جميع أنحاء العالم. جهاز استقبال **GPS** يحسب الموقع والوقت والسرعة من خلال معالجة إشارات مشفرة عبر القمر الصناعي (**satellite signals**) لتحديد المواقع. المهاجمون يعرفون أنه يتم توفر شبكات لاسلكية مجانا في كل مكان، وأيضا قد يكون هناك احتمال لوجود شبكة غير آمنة. المهاجمين يقومون عادة بإنشاء خرائط لشبكات الواي فاي المكتشفة، وإنشاء قاعدة بيانات مع إحصاءات تم جمعها بواسطة أدوات اكتشاف الواي فاي مثل **Netsurveyor**، **NetStumblers**، إلخ. **GPS** يستخدم لتتبع مواقع شبكات الواي فاي المكتشفة والاحداثيات يتم تحميلها على مواقع مثل **WIGLE**. المهاجمين يمكنهم مشاركة هذه المعلومات مع مجتمع المهاجمين أو بيعه لكسب المال.



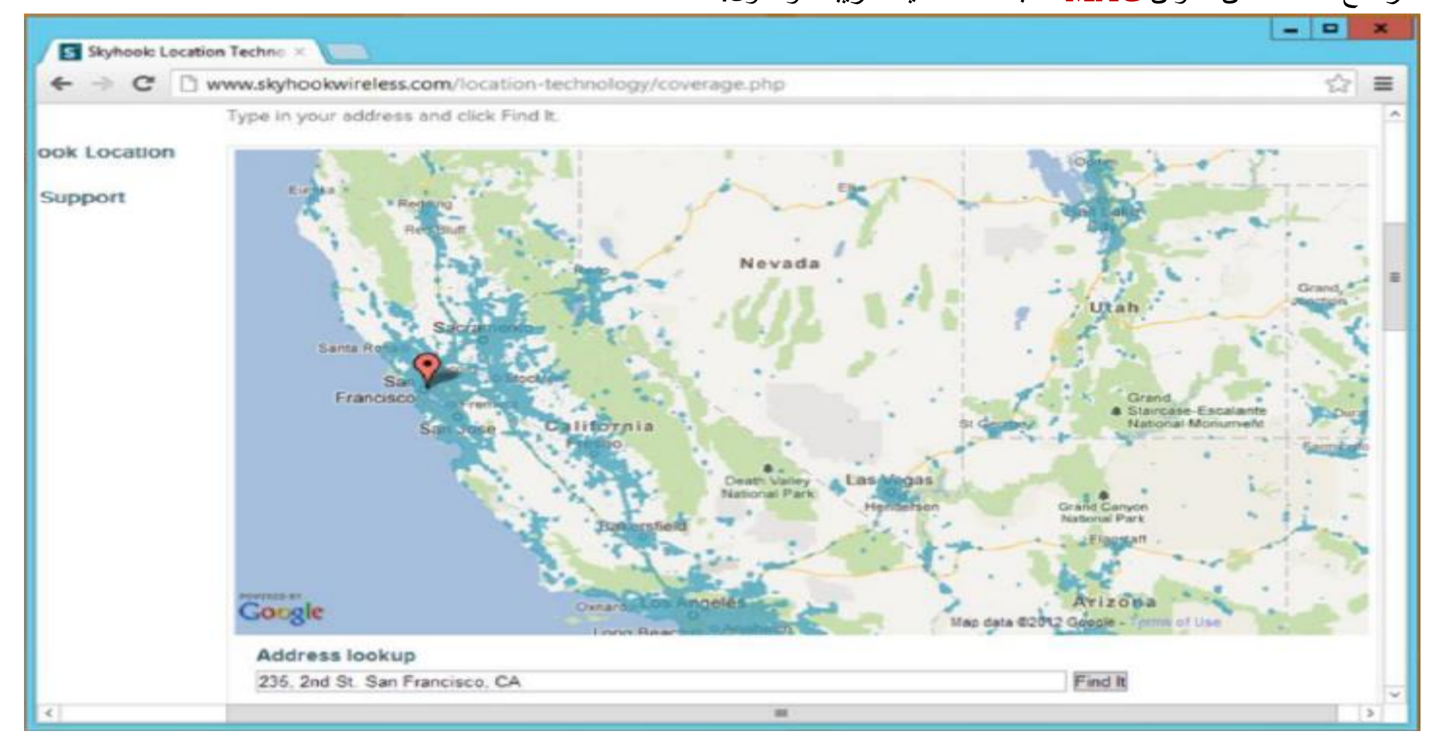
GPS Mapping Tool: WIGLE

المصدر: https://wigle.net
ويجلي يعزز مواقع ومعلومات عن الشبكات اللاسلكية على نطاق العالم إلى قاعدة بيانات مركزية، ويوفر جافا سهل الاستعمال، ويندوز، وتطبيقات ويب التي يمكنها تعيين، الاستعلام، وتحديث قاعدة البيانات عن طريق شبكة الإنترنت. باستخدام هذا يمكن للمستخدم إضافة شبكة اتصال لاسلكية إلى ويجلي من ملف **stumble** أو باليد عن طريق إضافة مواقع لشبكة موجودة. أنه يسمح للعثور على شبكة اتصال لاسلكية بالبحث أو تصفح الخريطة التفاعلية.

GPS Mapping Tool: Skyhook

المصدر : http://www.skyhookwireless.com

Skyhook's Wi-Fi Positioning System (WPS) يحدد الموقع استناداً إلى قاعدة بيانات **Skyhook's** العالمية الضخمة عن نقاط الوصول اللاسلكي المعروفة. فإنه يستخدم مزيجاً من نظام التتبع لتحديد المواقع (**GPS Tracking**) ونظام تحديد المواقع الواي فاي لتحديد موقع شبكة اتصال لاسلكية داخلي وفي المناطق الحضرية. حتى انه يكشف عن مواقع الجهاز المحمول على مسافة تتراوح بين 10 إلى 20 مترا مع مساعدة من عنوان **MAC** للشبكة اللاسلكية القريبة الوصول.



Wi-Fi Hotspot Finder: JiWire

المصدر: http://v4.jiwire.com

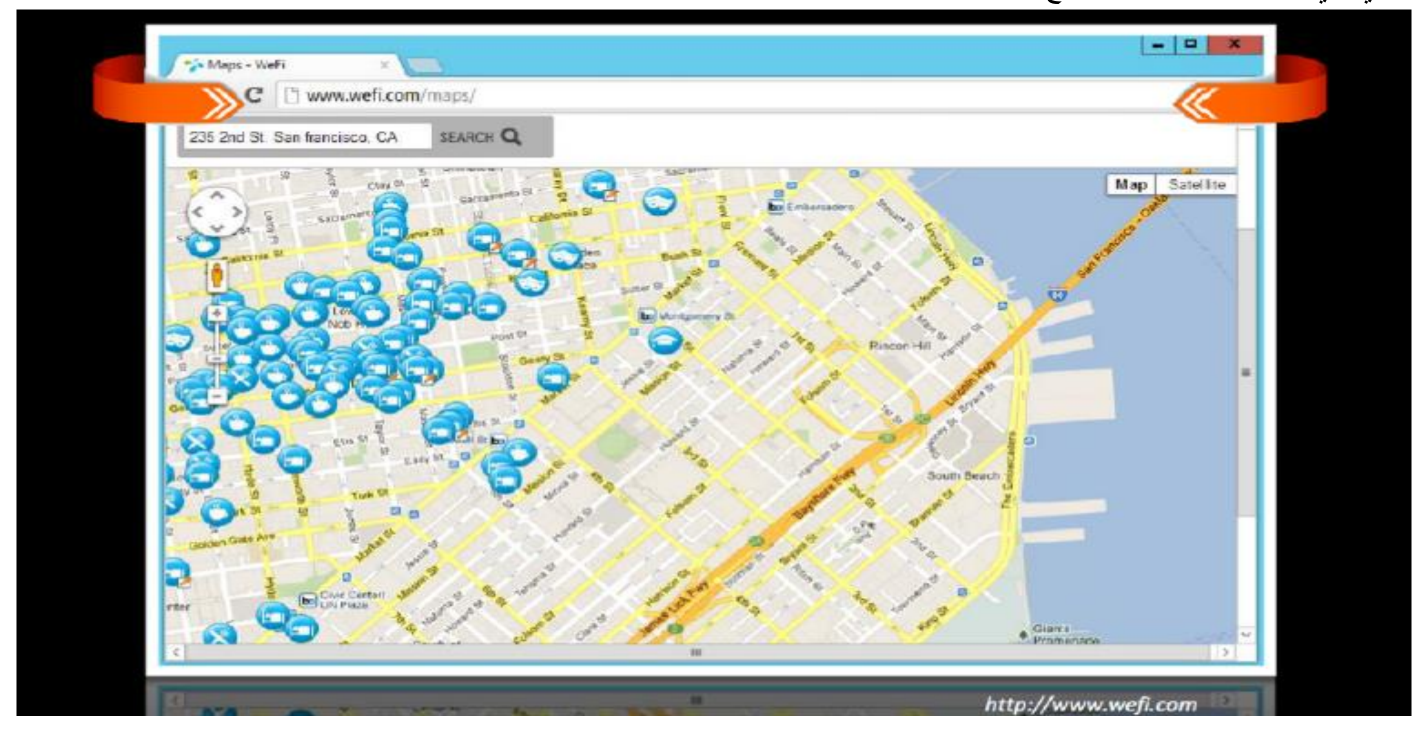
JiWire هو دليل لموقع نقاط الواي فاي مع أكثر من 788,723 من نقاط الواي فاي المجانية والمدفوعة في 145 بلدا وأنها تراقب الاتصالات اللاسلكية الخاصة بك. أنها طريقة بسيطة يمكنك من خلالها اكتشاف الإنترنت اللاسلكية التي يتناولها رجال الأعمال، فضلا عن الأشخاص الذين يعملون عن بعد. ويمكن بسهولة تصفح الأفراد للنقاط الواي فاي ليس فقط استناداً إلى موقعها، ولكن أيضا استناداً إلى أية معايير محددة سلفا مثل العنوان أو المدينة أو الرمز البريدي.



Wi-Fi Hotspot Finder: WeFi

المصدر: http://www.wefi.com

WeFi يوفر لك مواقع الواي فاي. يكتشف الاتصال الجديد، ويربطك تلقائياً مع واحد والذي هو الأفضل لاحتياجاتك. إصدار سطح المكتب سيقوم بإضافة نقاط الواي فاي التي تأسست حديثا بمساعدة النظام الخاص بك إلى قاعدة بيانات **WeFi** تلقائياً. يمكن أن تجد أقرب نقاط الواي فاي فيال محيط الخاص بك مع **WeFi**.



كيف اكتشاف شبكة الواي فاي باستخدام Wardriving

Wardriving واحد من التقنيات المستخدمة لاكتشاف شبكات **Wi-fi** المتوفرة في المنطقة المجاورة. ينبغي من أجل اكتشاف شبكات الواي فأي باستخدام **wardriving**، اتباع الخطوات التالية:

الخطوة 1: سجل مع موقع **WIGLE**، ومن ثم تحميل حزم الخريطة للمنطقة الخاص بك لعرض نقاط الوصول مرسومة على خريطة جغرافية.

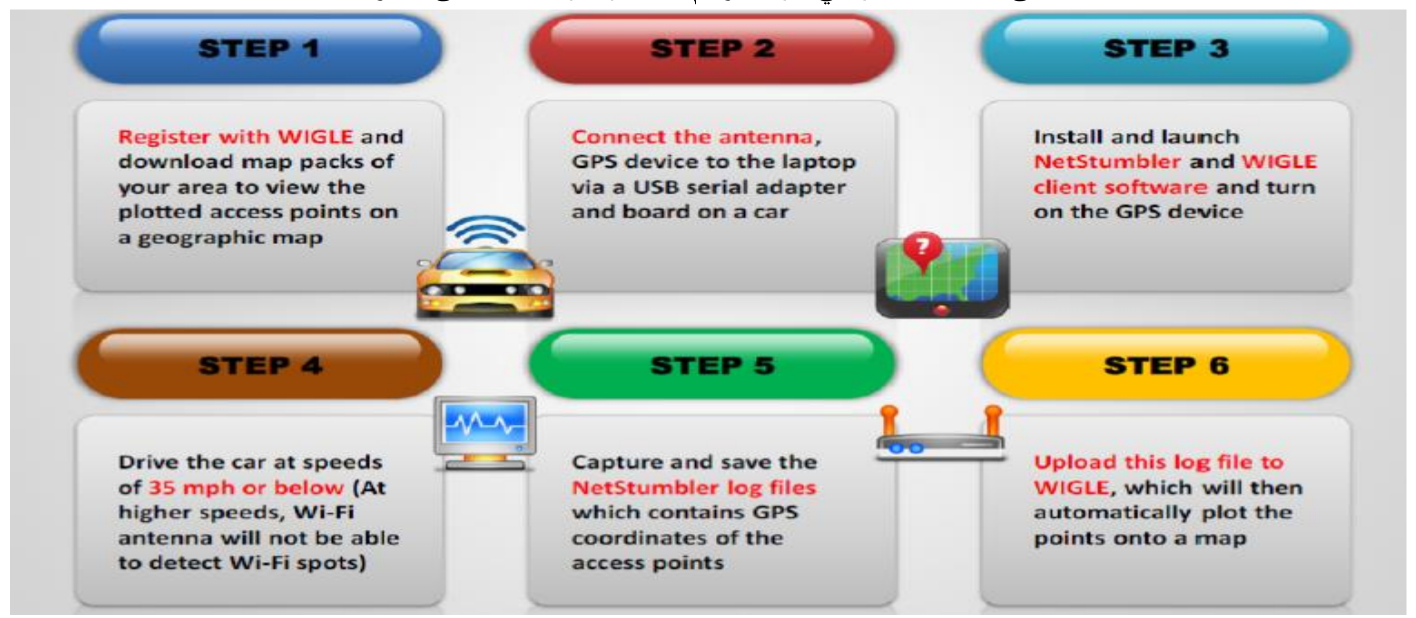
الخطوة 2: قم بوصل الهوائي وجهاز **GPS** بجهاز الكمبيوتر المحمول عن طريق **USB** ومن ثم وضعها في سيارتك.

الخطوة 3: تثبيت وتشغيل برنامج **NetStumbler** و**WIGLE** وتشغيل جهاز تحديد المواقع **GPS**.

الخطوة 4: قم بقيادة السيارة بسرعة 35 ميلا في الساعة أو أقل (في السرعات الأعلى، الهوائي لن يكون قادرة على الكشف عن نقاط وصول الواي فاي).

الخطوة 5: التقاط وحفظ ملفات السجل **NetStumbler** التي تحتوي على الإحداثيات لنقاط الوصول.

الخطوة 6: تحميل ملف السجل هذا على **WIGLE**، والتي سوف ترسم نقاط الوصول تلقائياً على الخارطة.



WIRELESS TRAFFIC ANALYSIS

كما ذكر سابقا، من ان الهدف من منهجية القرصنة اللاسلكية هو اختراق شبكة Wi-fi بغية الوصول غير المصرح به إلى موارد شبكة الاتصال. في هذه المنهجية، فان المرحلة الثالثة هي تحليل حركة المرور. حيث يقوم المهاجم بتحليل حركة المرور اللاسلكية قبل ارتكاب الهجمات الفعلية على شبكة الاتصال اللاسلكية. ويساعد تحليل حركة المرور اللاسلكية هذا المهاجم في تحديد نقاط الضعف في الشبكة المستهدفة.

تحليل حركة المرور اللاسلكية يقدم تقريرا مفصلاً عمن، ما، متى، وكيف نشاط شبكة الواي فاي. عملية تحليل حركة المرور تشمل العديد من المهام، مثل تطبيع البيانات، والتعرف على نمط حركة المرور، تشريح البروتوكول، وإعادة بناء جلسات عمل التطبيق. وهي تمكن المهاجمون من تحديد نقاط الضعف والضحايا في الشبكة اللاسلكية الهدف. ويساعد تحليل حركة المرور اللاسلكية على:

تحديد الثغرات الأمنية اللاسلكية

تحليل حركة مرور الشبكة اللاسلكية تمكن المهاجمون من تحديد نقاط الضعف والضحايا في الشبكة اللاسلكية الهدف. وهو يساعد في تحديد الاستراتيجية المناسبة للهجوم الناجح. بروتوكولات اللاسلكي فريدة من نوعها في الطبقة 2، وتسلسل حركة المرور يكون عبر الهواء، مما يجعل من السهل التنصت وتحليل الحزم اللاسلكية.

استطلاع الشبكة اللاسلكية

المهاجمين يقومون بتحليل الشبكة اللاسلكية لتحديد:

- بث **SSID**.



- وجود نقاط الوصول متعددة.
- إمكانية استرداد **SSIDs**.
- طريقة المصادقة المستخدمة.
- لوغاريتمية تشفير **WLAN**.

تأتي منتجات التقاط حزم الواي فاي وتحليلها في عدد من الأشكال. تتوفر العديد من الأدوات على الإنترنت التي تقوم بتحليل حركة المرور اللاسلكية. وتشمل أمثلة لأدوات تحليل حركة المرور اللاسلكية أداة **CommView**، **AirMagnet Wi-Fi Analyzer**، أداة الوايرشارك/**Pilot**، وأداة **OmniPeek**.

Wireless Cards and Chipsets

اختيار بطاقة الواي فاي مهم جداً نظراً لأدوات مثل **Aircrack-ng** و**KisMAC** تعمل فقط مع رقائق اللاسلكية محددة. فيما يلي بعض الاعتبارات التي يجب على المستخدم اتباعها من أجل اختيار البطاقة اللاسلكي الأمثل.

- **تحديد متطلبات الواي فاي الخاصة بك.**

إذا كنت تريد ببساطة الاستماع إلى حركة مرور شبكة الاتصال اللاسلكية أو كليهما الاستماع وحقن الحزم. فان الويندوز لديه القدرة على الاستماع فقط لحركة مرور شبكة الاتصال ولكن لا يمتلك القدرة على حقن حزم البيانات، في حين أن لينكس لديه القدرة على الاستماع الى الحزم والحقن. استناداً إلى هذه القضايا هنا عليك أن تقرر:

- أي من نظام التشغيل الذي تريد استخدامه.
- تنسيق الأجهزة مثل **PCMCIA** أو **USB**، وما إلى ذلك.
- والميزات مثل الاستماع أو الحقن أو كليهما.

- **معرفة قدرات بطاقة الشبكة اللاسلكية.**

كارت الشبكة اللاسلكية يشمل اثنين من المصنعين. واحد هو العلامة التجارية للبطاقة والآخر هو المصنع الذي أنشاء الرقاقات اللاسلكية داخل البطاقة. من المهم جداً أن ندرك الفرق بين هذين المصنعين. العلم بالشركة المصنعة للبطاقة والطراز لا يكفي لاختيار بطاقة الواي فاي. يجب ان يعرف المستخدم عن الرقاقة (**CHIPSET**) الموجودة داخل البطاقة. معظم الشركات المصنعة للشرائح لا تريد أن تكشف ما يستخدمونه داخل البطاقة الخاصة بهم، ولكنه مهم بالنسبة للمستخدمين ان يعرفوا هذا. العلم بالشركة المصنعة للرقاقات اللاسلكية يسمح للمستخدمين بتحديد نظام التشغيل الذي يدعم ذلك، برامج التشغيل المطلوبة، والقيود المرتبطة بها.

- **كيفية تحديد شرائح (CHIPSET) بطاقة الواي فاي**

أولاً يحتاج المستخدم لتحديد الشرائح (**CHIPSET**) اللاسلكية داخل البطاقة الذي يفكر ان يستخدمها لتلك الشبكات المحلية اللاسلكية. وفيما يلي الأساليب التي يمكن استخدامها لتحديد الشرائح (**CHIPSET**) داخل البطاقة اللاسلكية:

- البحث في الإنترنت.
- النظرة الى الملف التعريفي للكارت (**windows driver file names**). والذي هو غالباً يكون اسم الرقاقة أو **driver** قيد الاستخدام.
- راجع الصفحة الخاص بالشركة المصنعة.
- يمكنك أن ترى الرقاقة اللاسلكية من خلال النظر عليها حيث ان في بعض البطاقات مثل **PCI**. كثيراً ما يمكن ملاحظة رقم الرقاقة.
- يمكنك استخدام **FCC ID Search** للبحث عن معلومات مفصله عن الجهاز في حالة إذا كان الجهاز يتكون من رقم **FCC identification number** على الكارت نفسه. حيث أنه يعطي معلومات عن البطاقة عن الشركة المصنعة والطراز والشرائح.

في بعض الأحيان تغيير الشركات المصنعة للبطاقات الرقاقات داخل البطاقة مع الاحتفاظ بنفس رقم موديل البطاقة. وهذا عادة ما يسمى **card revision** او **card version** لذا، أثناء تحديد رقائق بطاقة الواي فاي، فيجب عليك ان تتأكد من تضمين **revision/version**. الرقائق تحدد طرق قد تختلف من نظام تشغيل واحد إلى آخر. قم بزيارة http://madwifi-project.org/wiki/Compatibility للحصول على معلومات التوافق.

- **التحقق من قدرات الرقاقة (CHIPSET)**

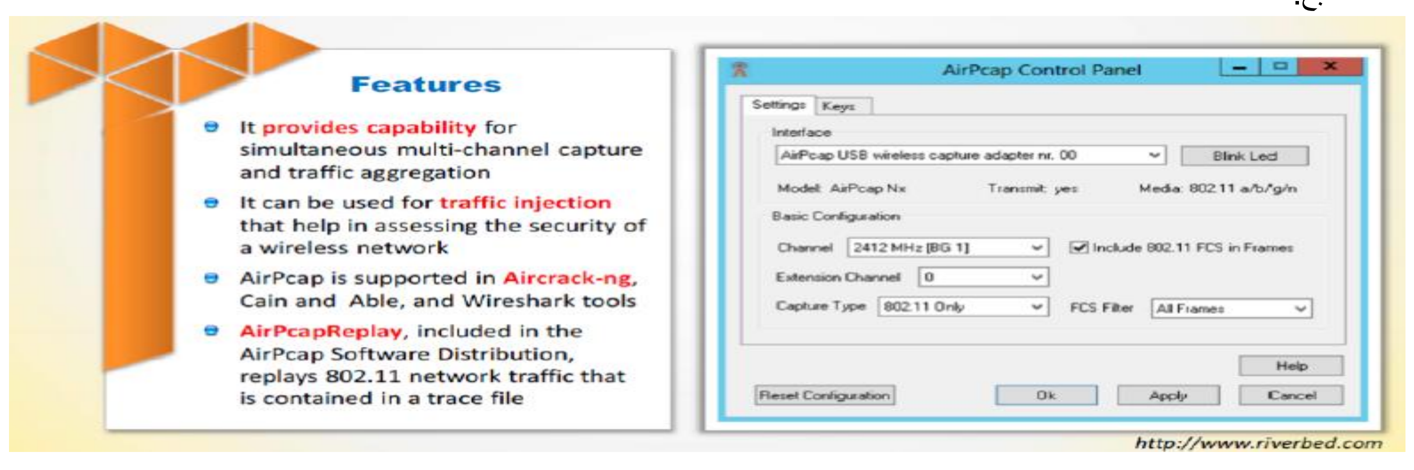
بعد اختيار بطاقة الواي فاي، فتأكد أو تحقق مما إذا كانت الرقاقة متوافقة مع نظام التشغيل الخاص بك والتحقق مما إذا كانت تلبي جميع الاحتياجات الخاصة بك. إذا كان الكارت غير متوافق مع نظام التشغيل أو لا يفي بمتطلبات المعايير، فقم بتغيير نظام التشغيل أو الرقائق اعتماداً على الاحتياجات.

- **تحديد برامج التشغيل (driver) والتصحيحات (patches) المطلوبة**

يمكنك تحديد برامج التشغيل المطلوبة للرقاقة باستخدام المقطع **driver** وتحديد التصحيحات المطلوبة لنظام التشغيل.
بعد تحديد جميع هذه الاعتبارات مع مجموعة الرقائق فان المستخدم يمكنه العثور على البطاقة التي تستخدم رقائق معينة مع مساعدة من قائمة التوافق الخاصة بالبطاقة.

Wi-Fi USB Dongle: AirPcap

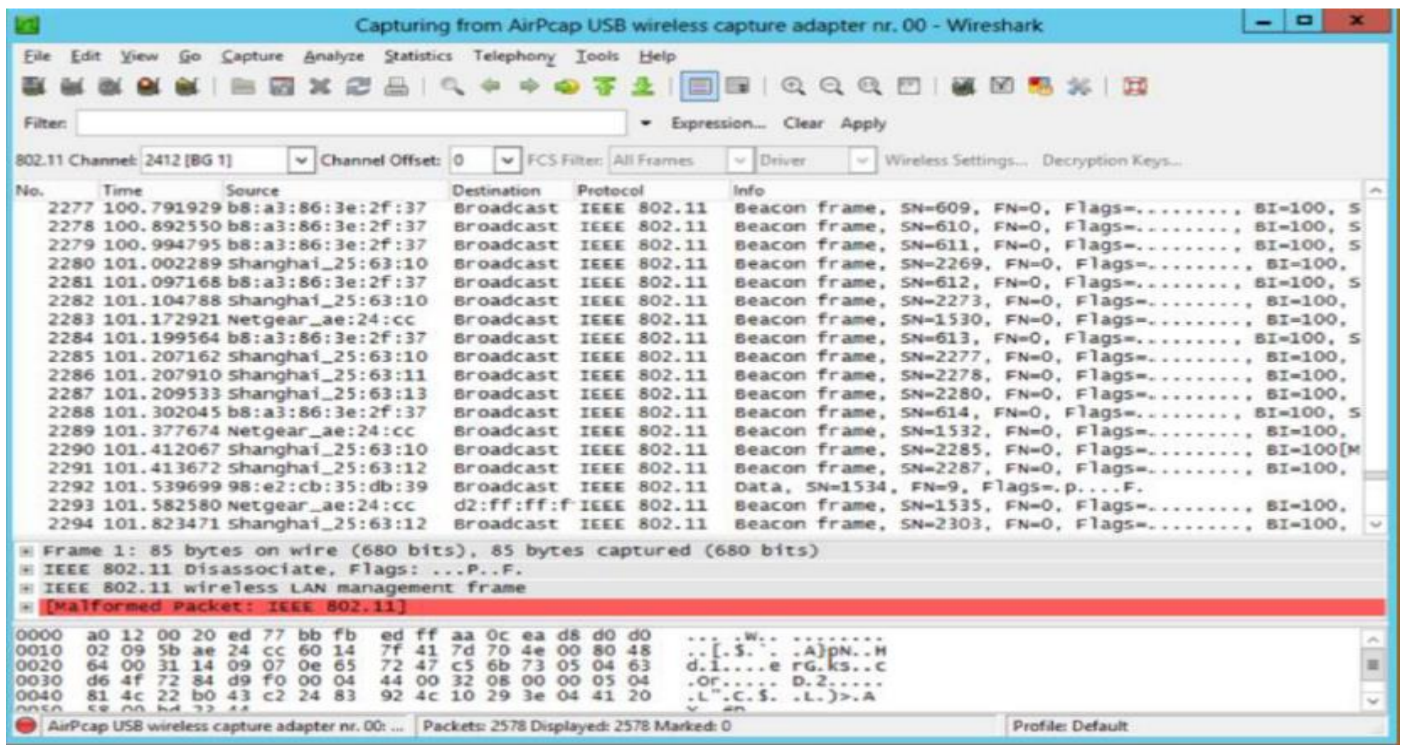
المصدر: http://www.riverbed.com
AirPcap يلتقط بيانات 802.11 كاملة، وإدارة ومراقبة الإطارات التي يمكن عرضها في الوايرشارك الذى يقدم تشريح متعمق للبروتوكول وقدرات التحليل. يمكن أن يعمل كافة محولات **AirPcap** في الوضع **passive** تماما. في هذا الوضع، محول **AirPcap** يمكنه التقاط كافة الإطارات التي يتم نقلها عبر القناة، ليس فقط الإطارات التي يتم توجيهها إليه. وهذا يشمل إطارات البيانات وإطارات التحكم وإدارة الإطارات. عند يكون أكثر من **BSS** واحد يتشاطرا نفس القناة، فإنه يمكن التقاط إطارات البيانات والمراقبة والإدارة من كل من **BSSs** التي يتقاسمان نفس القناة داخل نطاق محول **AirPcap**.
محولات **AirPcap** تلتقط حركة المرور على قناة واحدة في وقت واحد. القناة الإعداد هذه يمكن تغييرها باستخدام **AirPcap** ضمن لوحة التحكم، أو من مربع الحوار **Advanced Wireless Setting** في الوايرشارك. اعتماداً على قدرات محول **AirPcap** معين، يمكن تعيينها إلى أي قناة **802.11** صالحه لالتقاط الحزم. يمكن تكوينه لفك تشفير إطارات **WEP**. يمكن تكوين عدد عشوائي من المفاتيح في برنامج التشغيل في نفس الوقت، حيث أن برنامج التشغيل يمكنه فك تشفير حركة مرور نقطة وصول واحدة أو أكثر في وقت واحد. يدعم **WPA** و**WPA2** في الوايرشارك.
عند الرصد على قناة واحدة لا يكفي، يمكن توصيله العديد من محولات **AirPcap** في الكمبيوتر المحمول الخاص بك أو لوحة وصل **USB** متعددة وتوفير القدرة لالتقاط قنوات متعددة متزامنة وتجميع حركة مرور. برنامج تشغيل **AirPcap** يوفر الدعم لهذة العملية من خلال تكنولوجيا **Channel Aggregator** التي تصدر التقاط لتيارات من محولات **AirPcap** المتعددة كدفق التقاط واحد. يتكون **Multi-Channel Aggregator** من واجهة افتراضيه التي يمكن استخدامها مع الوايرشارك أو أي تطبيق أخر مستند إلى **AirPcap**. باستخدام هذه الواجهة، يتلقى التطبيق حركة المرور من كافة محولات **AirPcap** المثبتة، كما لو كانت قادمة من جهاز واحد. **Multi-Channel Aggregator** يمكن إعداده مثل أي جهاز **AirPcap**، ويمكن أن يكون له فك التشفير الخاص به والتحقق من **FCS**، وإعدادات فلترة الحزم.
يمكن استخدامه لحقن حركة المرور التي تساعد في تقييم أمان شبكة الاتصال اللاسلكية. معتمد من قبل الأدوات **Aircrack-ng**، **Cain and Able** والوايرشارك. **AirPcapReplay** ، تشمل في برمجيات **AirPcap**، للرد على حركة المرور 802.11 والتي تحتوى في ملف التتبع.



Wi-Fi Packet Sniffer: Wireshark with AirPcap

المصدر: https://www.wireshark.org
الوايرشارك هو محلل لبروتوكول شبكة الاتصال. وهو يتيح التقاط والتصفح التفاعلي لحركة المرور قيد التشغيل على شبكة اتصال كمبيوتر. هو بحكم الأمر الواقع قياسي عبر العديد من الصناعات والمؤسسات التعليمية.
الميزات:

- الالتقاط الحي والتحليل **offline**.
- منصة متعددة: يعمل على ويندوز، لينكس، **OS X**، سولاريس، **FreeBSD**، **NetBSD**، وغيره الكثير.
- يمكن تصفح بيانات الشبكة الملتقطة عبر واجهة المستخدم الرسومية، أو من خلال الأداة المساعدة تشارك **TTY**.
- **Display filters**.
- **VoIP analysis**.
- قراءة/كتابة العديد من تنسيقات ملفات الالتقاط المختلفة: **tcpdump (libpcap)**، **Pcap NG**، **Catapult DCT2000**، **Cisco Secure IDS iplog**، **Microsoft Network Monitor**، **Network General sniffer** (مضغوط وغير مضغوط)، **Sniffer Pro**، و**NetXray**، **NetScreen snoop**، **Novell LANalyzer**، **RADCOM**، **WLAN/LAN**، **shomiti/Finisar Surveyor**، وغيره الكثير.
- الملفات الملتقط يتم ضغطها بواسطة **gzip**.
- البيانات الحية يمكن قراءتها من **Ethernet**، **IEEE 802.11**، **PPP/HDLC**، **ATM**، **Bluetooth**، **USB**، **Token Ring**، **Frame Relay**، **FDDI**، وآخرون (اعتماداً على النظام الأساسي الخاص بك).
- يدعم فك تشفير العديد من البروتوكولات، بما في ذلك **IPsec**، **ISAKMP**، **Kerberos**، **SNMPv3**، **SSL/TLS**، **WEP** و**WPA/WPA2**. والعديد من المميزات الأخرى.



Wi-Fi Packet Sniffer: Cascade Pilot

المصدر: http://www.riverbed.com

Cascade Pilot Personal Edition (Wi-Fi pilot) هو محلل للشبكات السلكية واللاسلكية الذى احدث ثورة في استخدام الوايرشارك. متكامل تماما مع **Wireshark**، **Cascade Pilot Personal Edition** يعمل على زيادة هائلة في الكفاءة في تحديد وتشخيص مشاكل الشبكة.

Wi-Fi pilot يفعل الاتي:

- يقيس استخدام قناة لاسلكية من نقاط البيانات و**spectrum** في وقت واحد.
- يساعد في تحديد الشبكات اللاسلكية **rouge** والمحطات.
- يقدم تقارير مفصلة.



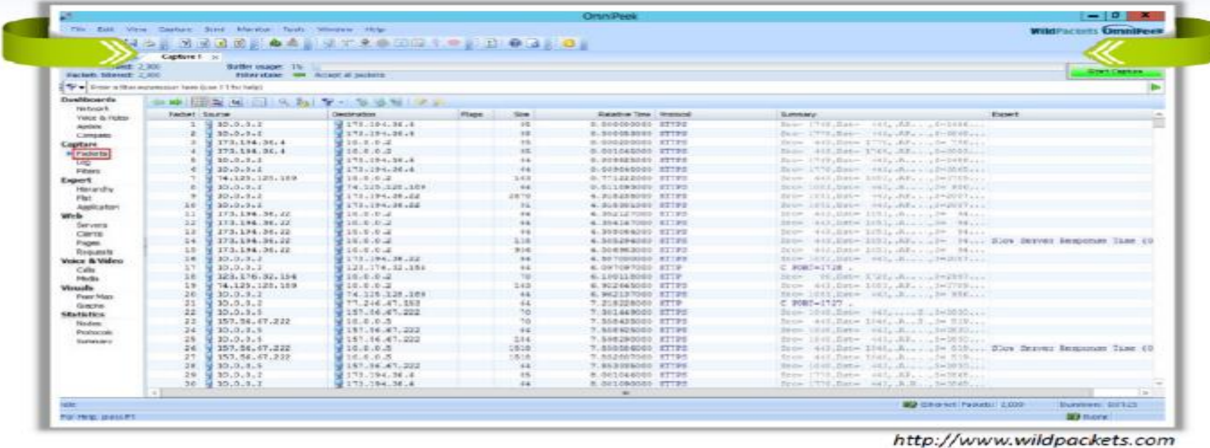
Wi-Fi Packet Sniffer: OmniPeek

المصدر: http://www.wildpackets.com

محلل الشبكة **OmniPeek** يوفر واجهة رسومية يمكن استخدامها من قبل المستخدمين لتحليل وحل مشكلات شبكات المؤسسة. أنه حتى يوفر الرؤية في الوقت الحقيقي "**Omreal-time visibility**" والتحليل في كل جزء من الشبكة من واجهة واحدة، بما في ذلك إيثرنت، **Gigabit**، **10 Gigabit**، **a/b/g/n802.11** اللاسلكية، **VoIP**، والفيديو للمكاتب البعيدة. استخدام واجهة المستخدم **OmniPeek** والنهج 'من أعلى إلى أسفل' لوضع تصور لحالة الشبكة، المستخدمين يمكنهم تحليل، الانتقال لأسفل وإصلاح اختناقات الأداء عبر شرائح متعددة في شبكة الاتصال.

يسلط الضوء على:

- إدارة أداء شبكة شاملة ورصد شبكات المؤسسة بأكملها، بما في ذلك قطاعات الشبكة في المكاتب البعيدة.
- شاشه تفاعلية لإحصائيات شبكة الاتصال الرئيسية في الوقت الحقيقي، وتجميع ملفات متعددة، والحفر وصولاً إلى الحزم باستخدام **Compass** لوحة تفاعلية.
- التفتيش العميق في الحزم.
- الدعم المتكامل لشبكة إيثرنت، **Gigabit**، **10 Gigabit**، **a/b/g/n802.11** اللاسلكية (بما في ذلك **3-stream**)، **VoIP**، **Video**، **MPLS**، و**VLAN**.
- الحفر لأسفل لفهم أي من العقد التي تتواصل العقد، أي من البروتوكولات والبروتوكولات الفرعية التي يتم إرسالها، وخصائص حركة المرور التي تؤثر على أداء الشبكة.
- تكملة رصد الصوت والفيديو عبر الإنترنت في الوقت الحقيقي بما في ذلك لوحة معلومات الوسائط المتعددة عالية المستوى واستدعاء بيانات السجل (**CDR**)، والإشارات ورصد أداء الوسائط وتحليلها.
- رصد أداء التطبيق والتحليل في سياق نشاط الشبكة الشاملة بما في ذلك القدرة على مراقبة وقت استجابة التطبيق، تأخير الشبكة ذهابا وإيابا، واستجابة الملقم، معاملات قاعدة البيانات بالثانية، وإحصاءات أخرى.
- بنية موسعة يمكن تكييفها بسهولة لمتطلبات الشبكة الفردية.



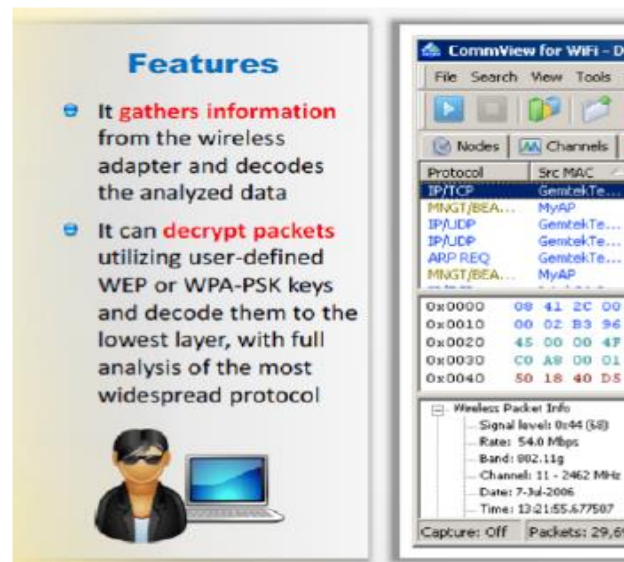


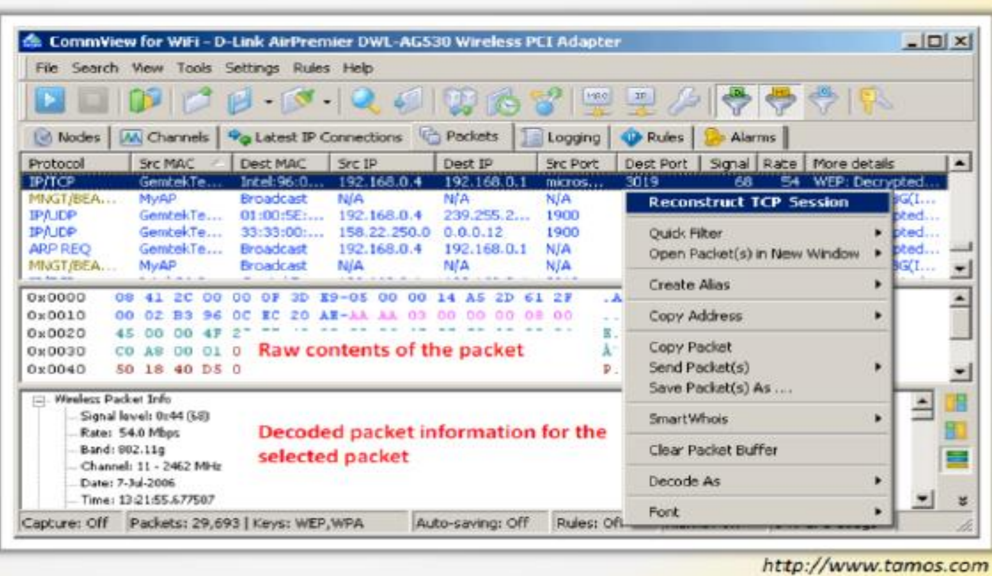

Wi-Fi Packet Sniffer: CommView for Wi-Fi

المصدر: http://www.tamos.com

CommView for Wi-Fi هو مراقب لشبكة الاتصال اللاسلكية، ومحلل لشبكات **802.11 a/b/g/n**. فإنه يلتقط كل حزمة في الهواء لعرض معلومات هامة مثل قائمة بنقاط الوصول والمحطات، الإحصاءات لكل عقده وبت لكل قناة، قوة الإشارة، قائمة باتصالات الشبكة، والبروتوكول ومخططات التوزيع وما إلى ذلك. بتوفير هذه المعلومات، فان **CommView for Wi-Fi** يمكن أن يساعد المستخدم في عرض وفحص الحزم وتحديد مشاكل شبكة الاتصال واستكشاف أخطاء البرامج والأجهزة. أنه يتضمن الوحدة النمطية **VoIP** للتحليل المتعمق، وتسجيل وتشغيل الاتصالات الصوتية **SIP** و **H.323**.

الحزم يمكن فك تشفيرها باستخدام مفاتيح **WEP** أو **WPA-PSK** المعرفة من قبل المستخدم، ويتم فك الشفرة وصولاً إلى طبقة أدنى. مع ما يزيد من 70 من البروتوكولات المعتمدة، ومحلل شبكة الاتصال هذا يسمح للمستخدمين بمشاهدة كل تفاصيل الحزمة التي تم التقاطها باستخدام بنية مثل الشجرة لعرض طبقات البروتوكول ورؤوس الحزم. بالإضافة إلى ذلك، يوفر المنتج واجهة مفتوحة لإضافة وحدات فك الترميز مخصصة. هذا التطبيق يعمل ضمن **Windows XP/2003/Vista/2008/7**، وتتطلب محول شبكة اتصال لاسلكية متوافقة.





ما هو تحليل الطيف (What Is Spectrum Analysis)؟

RF spectrum analyzers يقوم بفحص إرسال الراديو للواي فاي وقياس القوة (السعة) لإشارات الراديو و**RF pulses**، وتحويل هذه القياسات إلى تسلسلات رقمية. محللات الطيف (**spectrum analyzers**) توظف التحليل الإحصائي لتبيين الاستخدام الطيفي وقياس 'جودة الهواء'، وعزل مصادر الانتقال. محلل الطيف **RF spectrum analyzers** يستخدم من قبل فنيي **RF** لتثبيت وصيانة الشبكات اللاسلكية، وتحديد مصادر التدخل. تحليل الطيف اللاسلكي أيضا يساعد في الكشف عن الهجوم اللاسلكي، بما في ذلك هجمات الحرمان من الخدمة، هجمات المصادقة/فك التشفير، هجمات الاختراق وما إلى ذلك. محللات الطيف التقليدية هي معدات اختبار بنيت لهذا الغرض.

يمكن استخدام محلل الطيف اللاسلكي في العديد من الطرق. بالنظر في مهمة تحديد وتجنب التداخل بين الشبكات اللاسلكية والأجهزة التي تتنافس على نفس الترددات. إذا كنت تشك في تدخل الترددات اللاسلكية، قم بإيقاف **AP** أو المحطة المتأثرة، ثم قم باستخدام إحدى أدوات محلل الطيف اللاسلكي لمعرفة ما إذا كان أي جهاز يحيل ضمن نطاق ترددي معين. إذا كان هناك تداخل، فالمستخدمين يمكن القضاء على هذا التدخل بإعادة تكوين الشبكات المحلية اللاسلكية إلى قناة او تردد آخر لا تتداخل مع الترددات الأخرى في المنطقة المجاورة. أو آخر في محاولة لإزالة التداخل أو درع مصدر التدخل. أدوات تحليل الطيف مثل: **Wi-Spy Chanalyzer**، **AirMagnet Wi-Fi Analyzer**، **WifiEagle**، إلخ.

Wi-Fi Packet Sniffers

التنصت على حزم الواي فاي تساعدك على رصد وكشف واستكشاف الأخطاء وإصلاح مشاكل أداء الشبكة والتطبيق الحرجة. يتم سرد أدوات التنصت على حزمة الواي فأي المختلفة المتاحة بسهولة في السوق على النحو التالي:

Sniffer Portable Professional Analyzer available at http://www.netscout.com



Capsa WiFi available at http://www.colasoft.com
PRTG Network Monitor available at http://www.paessler.com
ApSniff available at http://www.monolith81.de
NetworkMiner available at http://www.netresec.com
Observer available at http://www.networkinstruments.com
WifiScanner available at http://wifiscanner.sourceforge.net
Mognet available at http://www.monolith81.de
Iperf available at http://iperf.sourceforge.net

LUNCH WIRELESS ATTACKS

بعد اكتشاف و**mapping**، وتحليل شبكة الاتصال اللاسلكية المستهدفة، حان الوقت لشن الهجمات عليها. العديد من الهجمات النشطة مثل هجمات **fragmentation**، هجمات **MAC spoofing**، هجمات الحرمان من الخدمة، هجمات **ARP poisoning**، إلخ يمكن إطلاقها ضد الشبكات اللاسلكية. الشرائح التالية تعطيك شرح مفصل عن كل الهجمات وكيفية إطلاقها.

Aircrack-ng Suite

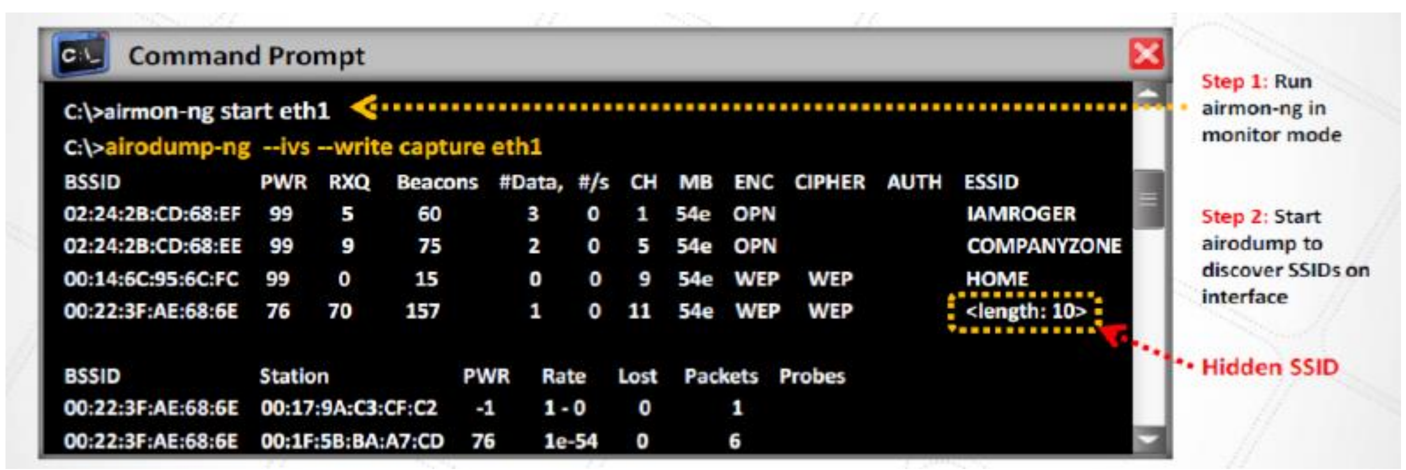
Aircrack-ng هي مجموعة من برمجيات الشبكة تتألف من جهاز الكشف، التنصت على الحزم، وكسر **WEP** و**WPA/WPA2-PSK** وتحليل الشبكات اللاسلكية 802.11. هذا البرنامج يعمل تحت لينكس وويندوز. أنه يعمل مع أي بطاقة شبكة لاسلكية الذي يدعم برنامج التشغيل فيه الوضع **monitoring mode** ويمكنه التنصت على حركة المرور **802.11a**، **802.11b**، و**802.11g**. هذه المجموعة تتضمن العديد من البرامج. القائمة التالية هي قائمة البرامج المضمنة في مجموعة أدوات **Aircrack-ng**:



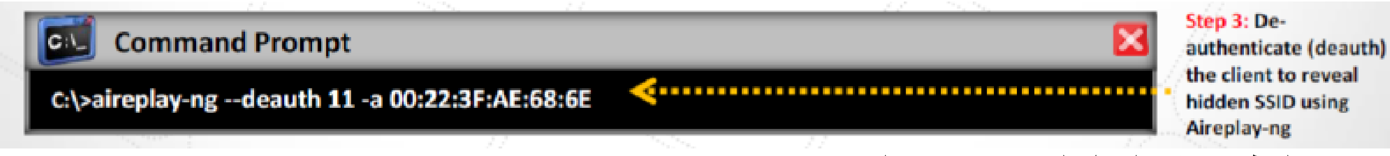
كيف الكشف عن SSIDs المخبأة

SSIDs المخبأة يمكن الكشف عنها باستخدام **Aircrack-ng suite**. وتنطوي العملية على الخطوات التالية:

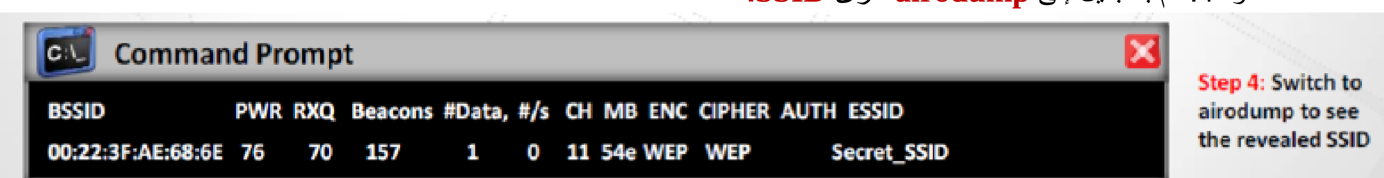
- الخطوة 1: تشغيل **airmon-ng** في الوضع **monitor mode**.
- الخطوة 2: بدء تشغيل **airodump** لاكتشاف **SSIDs** على الواجهة.



- الخطوة 3: المصادقة (**deauth**) مع العميل للكشف عن **SSID** المخفية باستخدام **Aireplay-ng**.



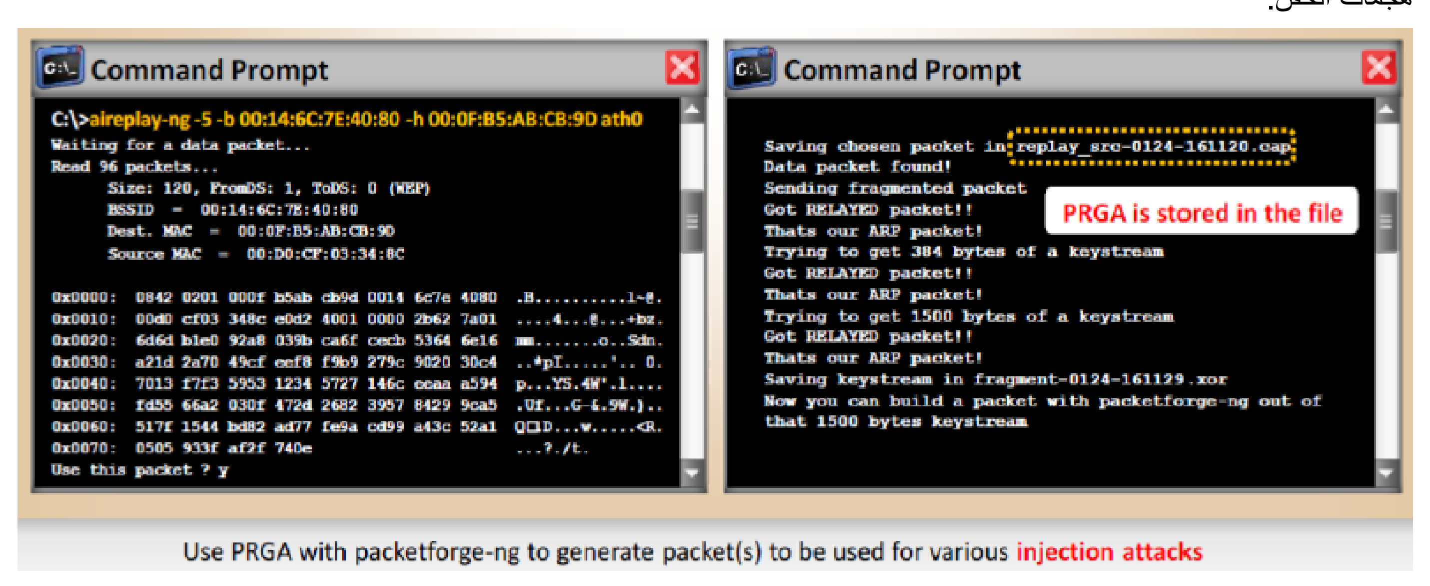
- الخطوة 4: قم بالتبديل إلى **airodump** لترى **SSID**.



Fragmentation Attack

عند نجاح الهجوم **Fragmentation**، فإنه يمكن الحصول على 1500 بايت من **PRGA** (***pseudo random generation algorithm***). هذا الهجوم لا يقوم باسترداد مفتاح **WEP** نفسها، ولكنه مجرد الحصول على **PGRA**. ثم يمكن استخدام **PGRA** لتوليد الحزم مع **packetforge-ng**، التي تستخدم بدورها في هجمات الحقن المختلفة. أنه يتطلب حزمة بيانات واحد على الأقل يتم تلقيها من نقطة الوصول من أجل الشروع في الهجوم.

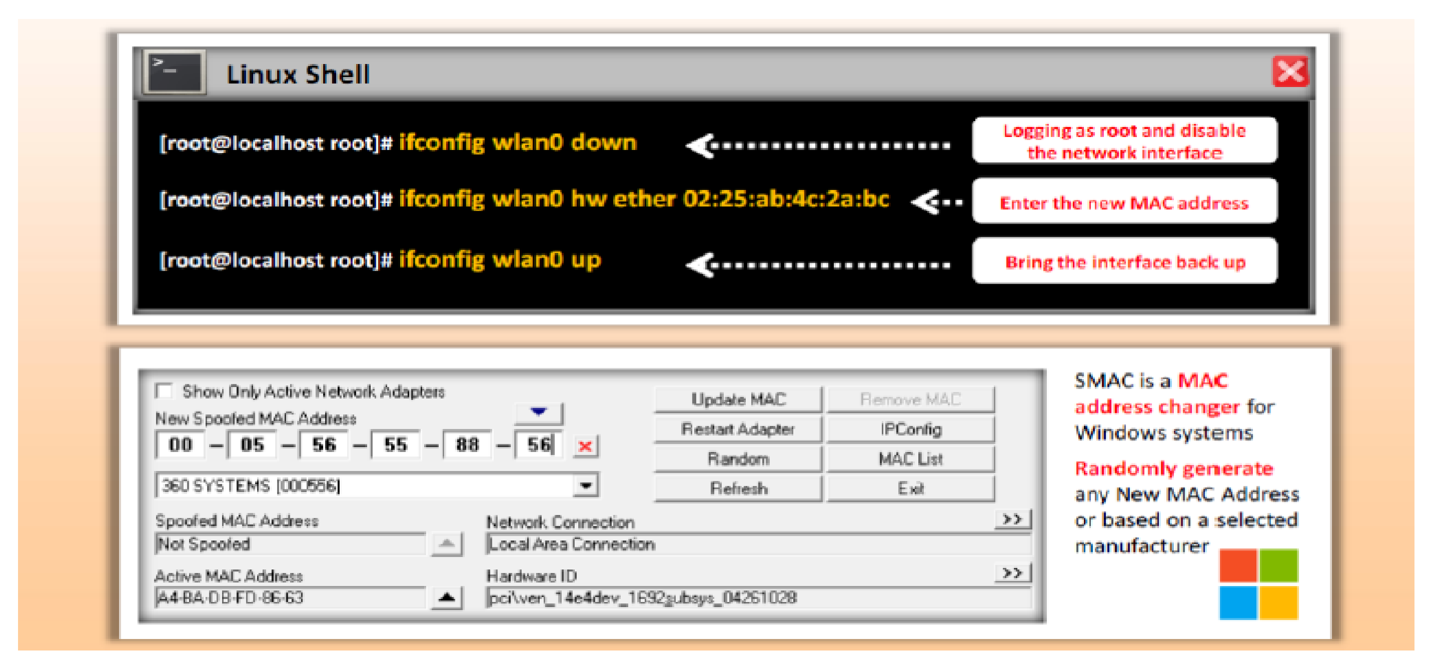
أساسا، البرنامج يحصل على كمية صغيرة من المفاتيح من الحزمة ثم محاولة إرسال حزم **ARP** و/أو **LLC packets** مع محتوى معروف الى نقطة الوصول (**AP**). يمكن جمع كمية أكبر من المعلومات من حزمة الإعادة (**replay packet**)، إذا تم ردد الحزمة بنجاح مرة أخرى بواسطة **AP**. وتتكرر هذه الدورة عدة مرات. يستخدم **PGRA** مع **packetforge-ng** لتوليد حزم يتم استخدامها لمختلف هجمات الحقن.



Use PRGA with packetforge-ng to generate packet(s) to be used for various injection attacks

كيف يمكنك إطلاق الهجوم MAC Spoofing Attack؟

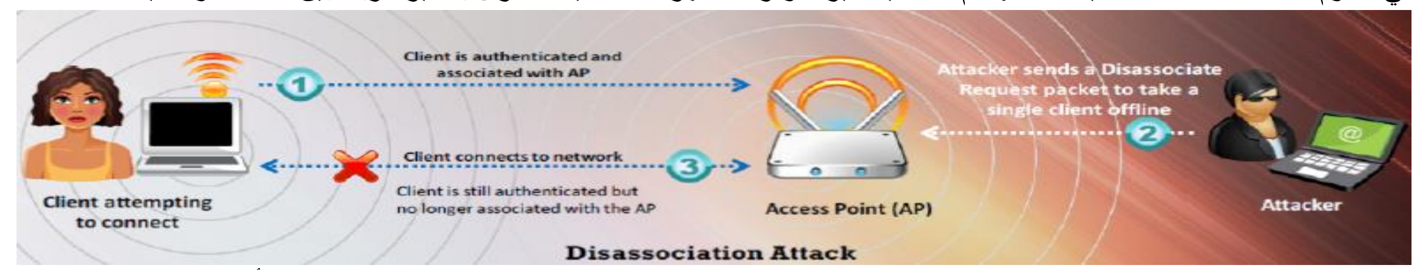
عنوان **MAC** هو معرف فريد تم تعيينه لبطاقة شبكة الاتصال. بعض الشبكات تقوم بفلترة عنوان **MAC** كتدبير أمني. في **MAC Spoofing** فان المهاجمين يقومون بتغيير عنوان **MAC** الى مستخدم تمت مصادقته لتجاوز فلترة **MAC** التي تم تكوينها في نقطة الوصول. من اجل القيام بـ **MAC Spoofing**، فان المهاجم ببساطة يكون في حاجة إلى تعيين القيمة التي تم إرجاعها من **ifconfig** إلى قيمة **hex** أخرى في الشكل **aa:bb:cc:dd:ee:ff**. **SMAC** هو مغير عنوان **MAC** لأنظمة **Windows**. يقوم بإنشاء أي عنوان **MAC** جديد عشوائياً أو استناداً إلى الشركة مصنعة محددة.



Denial of Service: Deauthentication and Disassociation Attacks

الشبكات اللاسلكية عرضه لهجمات الحرمان من الخدمة. وعادة ما تعمل هذه الشبكات في عصابات غير مرخصة ونقل البيانات يأخذ شكل إشارات الراديو. مصممين بروتوكول **MAC** يهدفون إلى الحفاظ على أنها بسيطة، ولكن لها مجموعتها الخاصة من العيوب التي هي أكثر جاذبية لهجمات **DoS**. إمكانية وقوع هجمات **DoS** على الشبكات اللاسلكية أكبر سبب العلاقة بين الطبقة الفيزيائية وطبقة البيانات، وطبقات الشبكة. يمكن تنفيذ هجمات **DoS** على الشبكات اللاسلكية باستخدام اثنين من التقنيات: هجمات **Deauthentication** وهجمات **Disassociation**.

في هجوم **Disassociation**، يجعل المهاجم الضحية غير متوفرة للأجهزة اللاسلكية الأخرى بتدمير الربط بين المحطة والعميل.



اما في هجمات **Deauthentication**، فان المهاجم يحاول اغراق المحطات مع **forged deauthentication** أو **disassociation** لقطع اتصال المستخدمين مع **AP**.



هجوم رجل فو الوسط (Man-in-the-Middle Attack)

هجوم الرجل في الوسط هو هجوم يحاول فيه المهاجم اعتراض أو قراءة أو تغيير المعلومات بين جهازي كمبيوتر. هجمات **MITM** ترتبط مع الشبكة المحلية اللاسلكية **802.11**، وكذلك مع أنظمة الاتصالات السلكية.

- **التنصت (Eavesdropping)**

التنصت سهل جدا في الشبكات اللاسلكية لأنه لا يوجد أي وسيط مادي مستخدم في الاتصال. حيث ان المهاجم الموجود في المنطقة التي تحتوي على الشبكة اللاسلكية يمكنه تلقي موجات الراديو عن الشبكة اللاسلكية دون بذل الكثير من الجهد أو العديد من الأدوات. حيث يمكنه فحص إطارات كامل البيانات المرسلة عبر شبكة الاتصال في الوقت الحقيقي أو تخزينها للتقييم الاحق.
من اجل منع الحصول على المعلومات الحساسة، ينبغي تنفيذ عدة طبقات من التشفير. **WEP**، **data-link encryption**، وضعت لهذا الغرض. إذا لم يتم استخدام إليه أمن مثل **IPSec**، **SSH**، أو **SSL** للإرسال، فان البيانات المرسلة سوف تصبح متاحه لأي شخص، وهو عرضه للهجوم من المتصنت مع هوائي.
ومع ذلك، يمكن اختراق **WEP** مع أدوات متاحة بحرية على شبكة الإنترنت. الوصول إلى البريد الإلكتروني باستخدام بروتوكولات **POP** أو **IMAP** محفوفة بالمخاطر نظراً لأن هذه البروتوكولات يمكنها إرسال البريد الإلكتروني عبر شبكة لاسلكية دون أي شكل من أشكال التشفير. يمكن تسجيل مما يقرب من الغيغا بايت لحركة المرور المحمية بواسطة **WEP** من اجل السعي فيما بعد من اجل كسر الحماية.

- **التلاعب (Manipulation)**

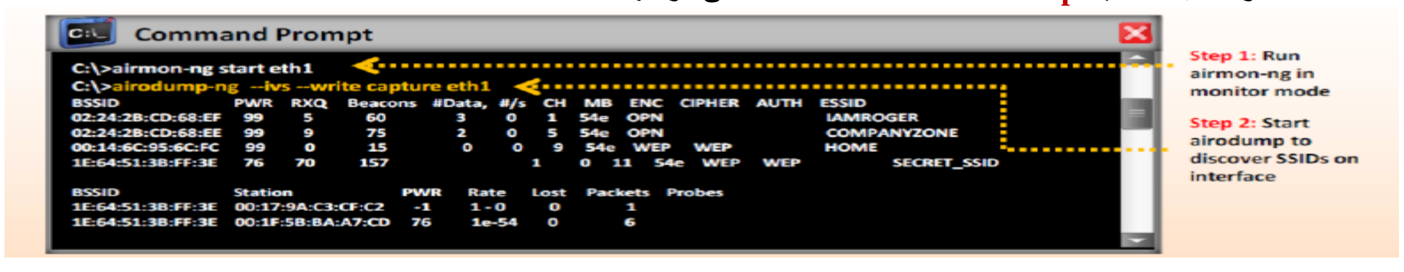
التلاعب هو المستوى التالي من التنصت. يحدث التلاعب في الوصلة اللاسلكية عندما يكون مهاجم قادراً على تلقي البيانات المشفرة للضحية والتلاعب بها، وإعادة إرسال البيانات التي تم تغييرها للضحية. وبالإضافة إلى ذلك، يمكن للمهاجم اعتراض الحزم مع البيانات المشفرة وتغيير عنوان الوجهة من أجل توجيه هذه الحزم عبر شبكة الإنترنت. ويوضح الشكل التالي شرح خطوة بخطوة لهجوم رجل في الوسط:



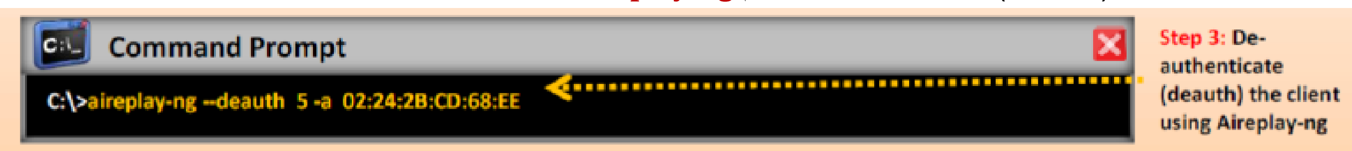
- **هجوم MITM باستخدام Aircrack-ng**

Aircrack-ng هي مجموعة من برمجيات الشبكة تتألف من جهاز كشف، التنصت على الحزم، وأداة لكسر تشفير **WEP** و**WPA/WPA2-PSK**، واداة لتحليل شبكات الاتصال اللاسلكية 802.11. يمكن استخدامها لتنفيذ هجمات رجل في الوسط على الشبكات اللاسلكية. للقيام بهجوم **MITM** في شبكات **WLAN** باستخدام **Aircrack-ng** يجب اتباع الخطوات التالية:

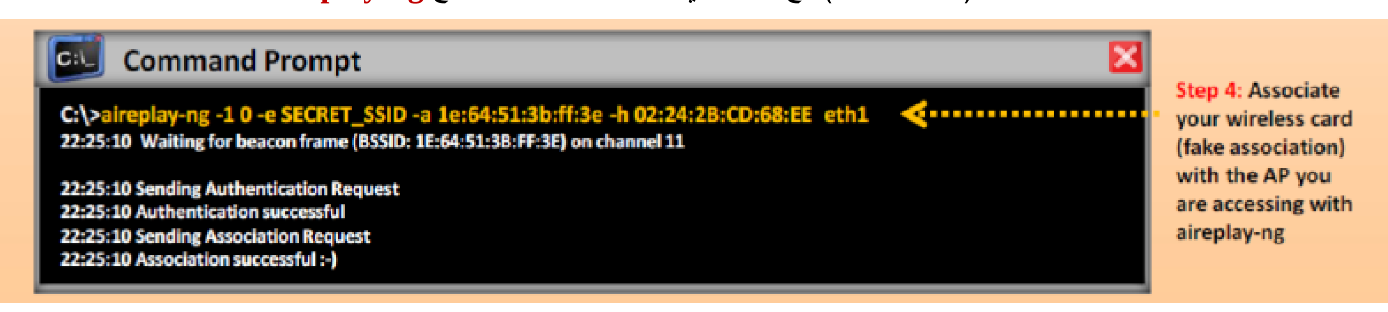
- الخطوة 1: تشغيل **airmon-ng** في وضع المراقبة.
- الخطوة 2: بدء تشغيل **airodump** لاكتشاف **SSIDs** على الواجهة.



- الخطوة 3: إزالة (**deauth**) مصادقة العميل باستخدام **Aireplay-ng**.

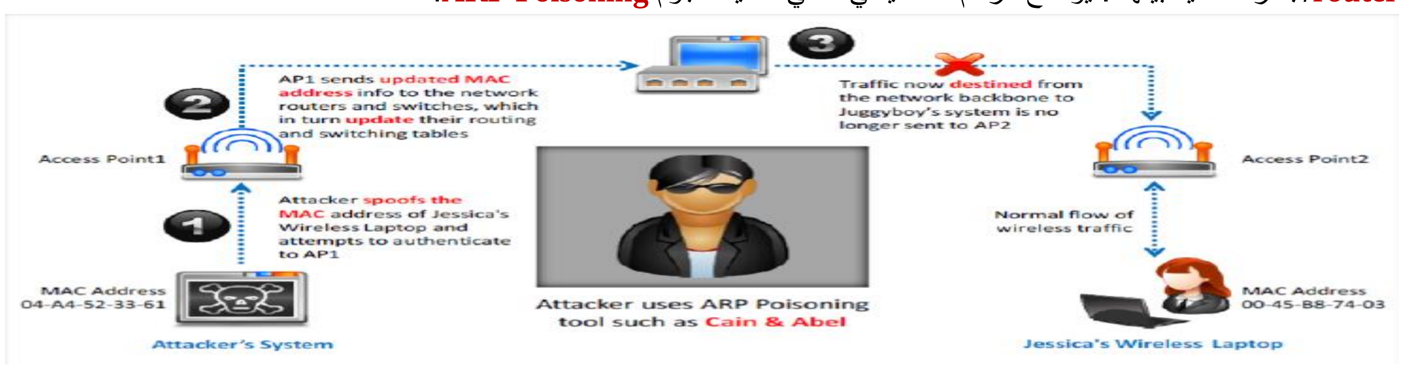


- الخطوة 4: إقران بطاقة لاسلكية (رابطة وهمية) مع AP الذي تحاول الوصول إليها مع **Aireplay-ng**.



Wireless ARP Poisoning attack

ARP يستخدم لتحديد عنوان **MAC** لنقطة الوصول إلى عنوان **IP** الذي هو معروف. عادة **ARP** لا يمتلك ميزة التحقق التي يمكن أن تقول إن الردود تأتى من المضيفين الصالح أو أنه يتلقى استجابة مزورة. **ARP Poisoning** هو أسلوب هجوم الذي يستغل عدم وجود ميزة التحقق هذه. في هذا الأسلوب يتم حفظ **ARP cache** في نظام التشغيل مع عناوين **MAC** الخاطئة. يمكن أن يتحقق هذا عن طريق إرسال حزمة **ARP Replay** التي شيدت مع عنوان **MAC** غير صحيح.
هجوم **ARP Poisoning** له أثره على كافة الأجهزة المضيفة الموجودة في الشبكة الفرعية. جميع المحطات المرتبطة بالشبكة الفرعية المتأثرة بهجوم **ARP Poisoning** يكون ذات ضعف كما معظم **AP** التي هي بمثابة جسور لطبقة **MAC**. كافة المضيفين المتصلين بال **Switch** أو **hub** معرضه لهجمات **ARP Poisoning** إذا كانت نقطة الوصول متصلة مباشرة بهذا ال **Switch** أو **hub** دون أي جهاز **router**/جدار الحماية بينهما. يوضح الرسم التخطيطي التالي عملية هجوم **ARP Poisoning**:



نقطة الوصول المارقة (Rouge Access Point)

نقاط وصول المارقة (**APs**) هي نقاط الوصول اللاسلكية المثبتة على شبكة اتصال بدون إذن، وليست تحت إدارة مسؤول شبكة الاتصال. نقاط الوصول المارقة هذه تفتقر إلى الضوابط الأمنية المقدمة ل **APs** المأذون بها من شبكة الاتصال، وبالتالي توفر الوصول المستتر (**backdoor**) إلى شبكة الاتصال لأي شخص يتصل بنقطة الوصول المارقة هذه. للوصول المستتر الى الشبكة من خلال جهاز **AP** المارق، فان المهاجم يجب عليه اتباع الخطوات التالية:

- اختيار الموقع المناسب للدخول (**plug**) الى نقطة الوصول المارقة التي تتيح أقصى قدر من التغطية من نقطة الاتصال الخاصة بك.
- تعطيل بث **SSID** (الوضع الصامت)، وأية ميزات إدارة لتجنب الكشف.
- وضع نقطة الوصول خلف جدار حماية، إذا كان ذلك ممكناً، لتجنب فاحصات الشبكة.
- انشاء نقطة وصول دخيلة لفترات أقصر.

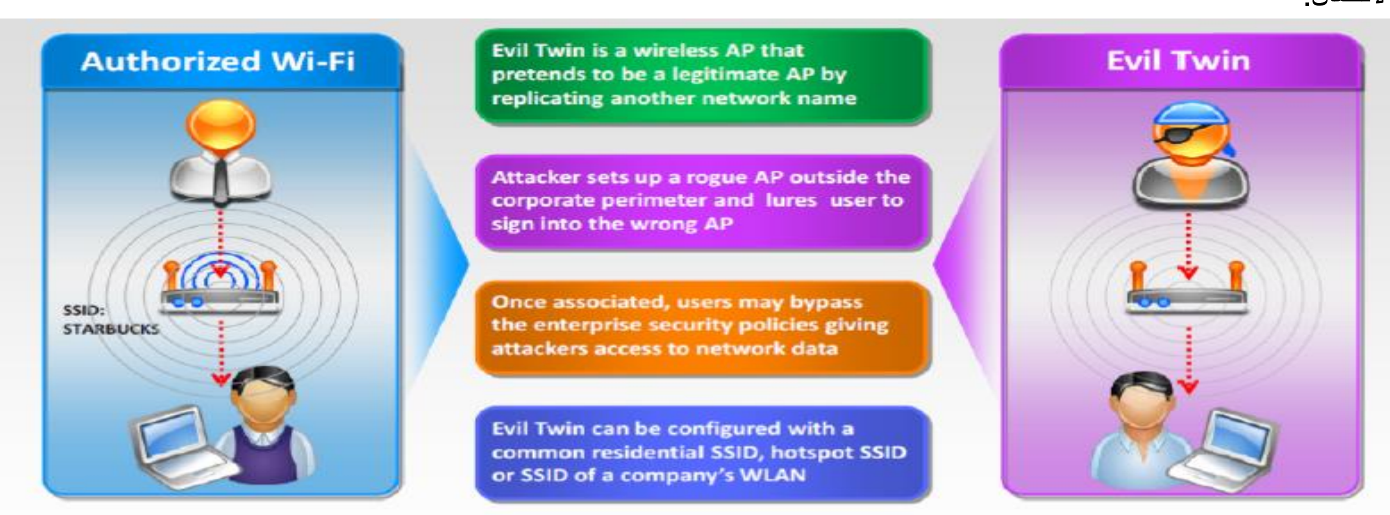
السيناريوهات المثيرة للاهتمام عند اعداد او تثبيت rouge AP:

- **Compact, pocket-sized rogue AP device plugged into an Ethernet port of corporate network:** نقاط الوصول المارقة المدمجة الصغيرة الحجم متاحة بسهولة في السوق. نتيجة لحجمها المضغوط. فأنه يمكن جلبها إلى موقع معين دون أي جهود ويمكن إخفاؤها بسهولة. أيضا، نقاط الوصول هذه تتطلب طاقة منخفضة جدا. وبالتالي، فإنها يمكن أن تعمل بالطاقة حتى من البطارية لفترات طويلة.
- **Rogue AP device connected to corporate networks over a Wi-Fi link:** نقاط الوصول المارقة يمكن أيضا ان تكون جهاز متصل بشبكة عبر ارتباط لاسلكي. وهذا ممكن عندما تكون الشبكة المستهدفة لديها تغطية الواي فأي. إخفاء هذا الجهاز **AP** المارق سهله كما في جهاز **AP** المتصل لاسلكياً بالشبكة المأذون بها. هذا يلغي الحاجة إلى منفذ إيثرنت غير مستخدم في الشبكة المستهدفة، ولكن تركيب جهاز **AP** المارق لاسلكياً يتطلب بيانات اعتماد الشبكة المستهدفة. ينبغي على المهاجم استخدام **Wi-Fi Ethernet Bridge** للاقتران مع جهاز **AP** عادي بغية الاتصال بالشبكة المستهدفة.
- **USB-based rogue AP device plugged into a corporate machine:** أحد أجهزة **rouge AP** المستندة إلى **USB** تكون عموما موصلة بجهاز **windows** يتصل بالشبكة المستهدفة أما سلكي أو لاسلكي. الوصول إلى شبكة الاتصال للجهاز يمكن تقاسمها مع جهاز **rouge AP**. هذا يلغي الحاجة إلى منفذ إيثرنت غير مستخدم ووثائق التفويض مع شبكة الواي فاي الهدف من أجل إعداد جهاز **AP** المارق.
- **Software-based rogue AP running on a corporate Windows machine:** في هذا السيناريو، ليس هناك الحاجة إلى أي جهاز **AP** مادي منفصل كـ **rouge AP** الذى يتم إعداده في البرنامج نفسه على المحول اللاسلكي كجزء من توصيل الشبكة المستهدفة. وهذا ممكن من خلال القدرة اللاسلكية الافتراضية في نظام التشغيل ويندوز، ويندوز 7.

Evil Town

Evil Town هي نقطة وصول لاسلكية التي تتظاهر بأنها جهاز **AP** مشروع بتقليد اسم شبكة اتصال آخر. وهو يشكل خطرا واضحا وقائماً للمستخدمين اللاسلكيين في شبكات **Wlan** القطاعين العام والخاص. يقوم المهاجم بإعداد جهاز **AP** مارق خارج محيط الشركات وخداع المستخدم لتسجيل الدخول إلى نقاط الوصول الخاطئة. المهاجم يمكنه استخدام أدوات مثل **KARMA** التي تراقب المحطة لإنشاء **Evil Town**. يمكنها اعتماد أي **SSID** المستخدمة بشكل شائع كـ **SSID** الخاص به من أجل جذب المستخدمين. أو يمكن تكوين **Evil Town** مع **SSID** مشتركة، **SSID hotspot** أو **SSID** للشبكة المحلية اللاسلكية للشركة. يمكن رصد المستخدم المشروع مع مختلف أدوات حتى مع **AP**، التي لا تقم بإرسال **SSID** في **probe request** يمكن توجيهها.

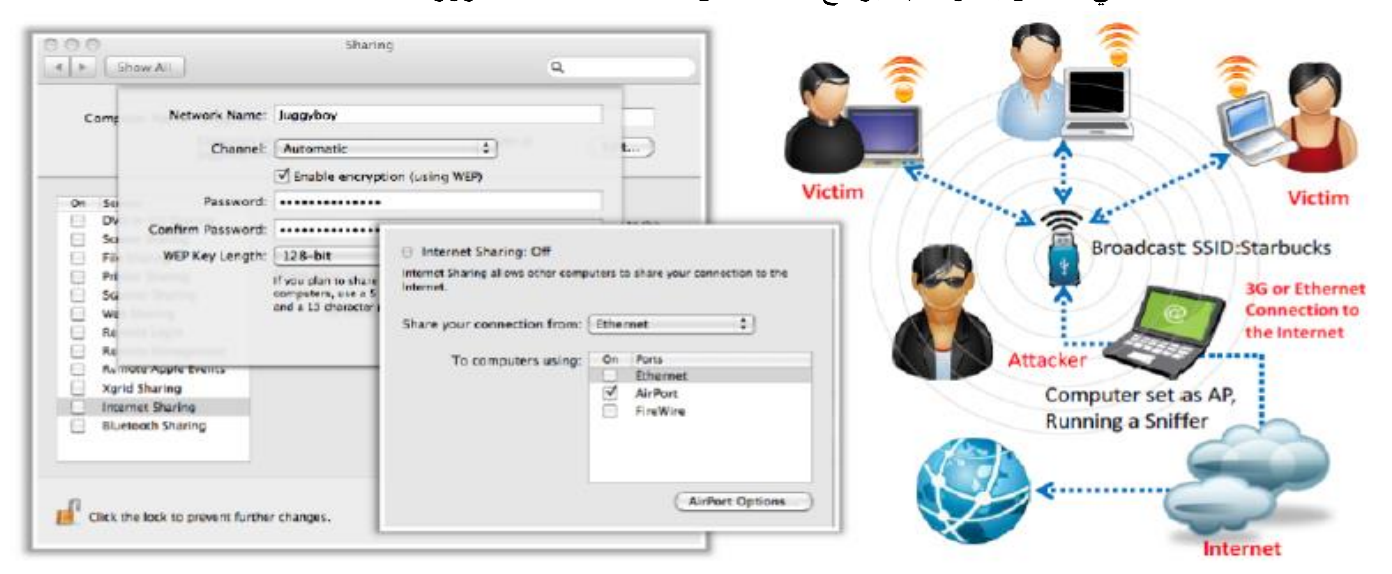
محطات الشبكات اللاسلكية عادة تتصل بنقاط الوصول المحددة استناداً إلى **SSID** لها وقوة الإشارة وأيضا المحطات يمكنها إعادة الاتصال تلقائياً إلى أي **SSID** التي تم استخدامها في الماضي. هذه المسائل يسمح للمهاجمين لخداع المستخدمين الشرعيين بسهولة فقط بوضع **Evil Town** قرب الهدف. بمجرد الارتباط، المستخدمين يمكنهم تجاوز نهج أمان المؤسسة بإعطاء المهاجمين الوصول إلى بيانات شبكة الاتصال.



▪ كيفية اعداد نقاط وصول مزيفه (How to Set Up a Fake Hotspot (Evil Twin))؟

Hotspot المتوفرة في المنطقة قد لا تكون دائماً **AP** مشروعة. قد يكون هناك احتمال ان تكون **evil town** شنت من قبل المهاجم لتتظاهر بأنها نقطة وصول مشروعة. من الصعب التفريق بين نقطة مشروعة ونقطة **evil town** حيث ان **evil town** تتظاهر بأنها نقاط وصول المشروعة. فعلى سبيل المثال، المستخدم يحاول تسجيل الدخول، ويرى اثنين من نقاط الوصول. واحد مشروعة، بينما الآخر وهمية متطابقة (**evil town**). يختار الضحية واحدة؛ إذا أنها وهمية، يحصل المهاجم على معلومات تسجيل الدخول والوصول إلى الكمبيوتر. وفي الوقت نفسه، لا يذهب المستخدم الى أي مكان. أنه ربما يعتقد أنها كانت مجرد محاولة تسجيل دخول فاشله بشكل عشوائي. وفيما يلي الخطوات التي توضح عملية إعداد أو تركيب نقطة وهمية (**evil town**):

- سوف تحتاج إلى جهاز كمبيوتر محمول مع اتصال بالإنترنت (اتصال سلكي أو الجيل الثالث g3) ونقطة وصول.
- تمكين **Internet Connection Sharing** في **Windows 7** أو **Internet Sharing** في **Mac OS X**.
- بث الاتصال اللاسلكي الخاص بك وتشغيل برامج التنصت من اجل التقاط كلمات المرور.



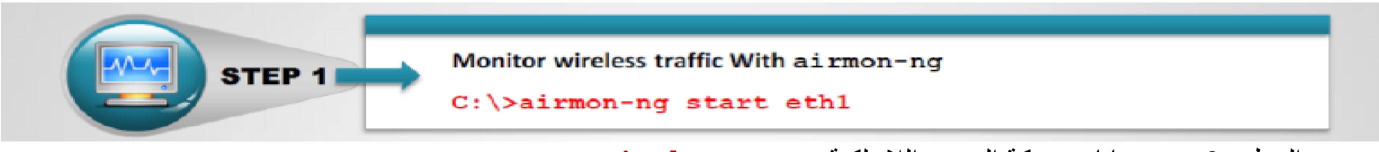
CRACK WI-FI ENCRYPTION

الشبكة اللاسلكية، ينبغي عليك تحديد التشفير المستخدم من قبل الشبكات المحلية اللاسلكية ومن ثم كسر هذا التشفير.

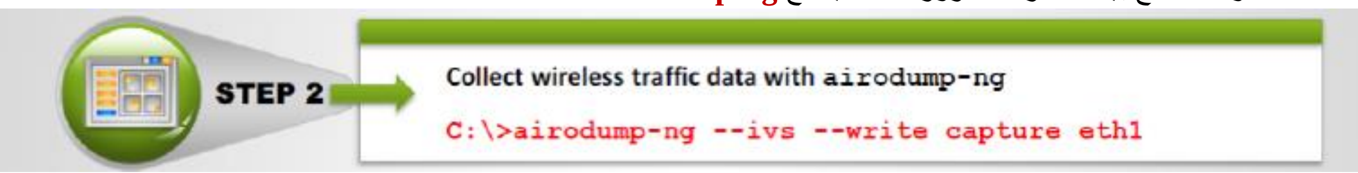
كيفية كسر تشفير WEP باستخدام Aircrack

WEP هي خوارزمية أمن مكسورة لشبكات الاتصال اللاسلكية 802.11. فإنه يهدف إلى توفير سرية البيانات في الشبكات اللاسلكية. المهاجم يرغب في كسر مفتاح التشفير هذا لاقتحام الشبكات اللاسلكية. هذا **WEP** به نقاط الضعف التي يمكن استغلالها بسهولة، وهكذا، يمكن كسر مفتاح **WEP**. تشرح الخطوات التالية عملية تكسير **WEP** باستخدام أداة **Aircrack**.

- الخطوة 1: رصد حركة المرور اللاسلكية مع **airmon-ng**.



- الخطوة 2: جمع بيانات حركة المرور اللاسلكية مع **airodump-ng**.



- الخطوة 3: إقران البطاقة اللاسلكية مع نقطة الوصول التي تحاول الوصول إليها مع **aireplay-ng**.

STEP 3

Associate your wireless card with the AP you are accessing with aireplay-ng

```
C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e
-h a7:71:fe:8e:d8:25 eth1
```

- الخطوة 4: بدء حقن الحزمة مع **aireplay-ng**.

STEP 4

Start packet injection with aireplay-ng

```
C:\>aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h
a7:71:fe:8e:d8:25 eth1
```

- الخطوة 5: فك تشفير مفتاح **WEP** مع **Aircrack-ng**.

STEP 5

Decrypt the WEP Key with aircrack-ng

```
C:\>aircrack-ng -s capture.ivs
```

Command Prompt

```
C:\>airmon-ng start eth1
C:\>airodump-ng --ivs --write capture eth1
BSSID              PWR  RXQ  Beacons  #Data, #/s  CH  MB   ENC  CIPHER  AUTH  ESSID
02:24:2B:CD:68:EF  99   5    60       3      0    1   54e  OPN                IAMROGER
02:24:2B:CD:68:EE  99   9    75       2      0    5   54e  OPN                COMPANYZONE
00:14:6C:95:6C:FC  99   0    15       0      0    9   54e  WEP  WEP           HOME
1E:64:51:3B:FF:3E  76   70   157      1      0    11  54e  WEP  WEP           SECRET_SSID

BSSID              Station            PWR  Rate  Lost  Packets  Probes
1E:64:51:3B:FF:3E  00:17:9A:C3:CF:C2  -1   1-0   0     1
1E:64:51:3B:FF:3E  00:1F:5B:BA:A7:CD  76   1e-54 0     6
```

Step 1: Run airmon-ng in monitor mode

Step 2: Start airodump to discover SSIDs on interface and keep it running. Your capture file should contain more than 50,000 IVs to successfully crack the WEP key.

Command Prompt

```
C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:25:10  Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E) on channel 11

22:25:10 Sending Authentication Request
22:25:10 Authentication successful
22:25:10 Sending Association Request
22:25:10 Association successful :-)
```

Target SSID — Target MAC address

Step 3: Associate your wireless card with target access point

Command Prompt

```
C:\>aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:30:15  Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E)

Saving ARP requests in replay_arp-0219-123051.cap
You should also start airodump-ng to capture replies
Read 11978 packets (got 7193 ARP requests), sent 3902 packets...
```

Step 4: Inject packets using aireplay-ng to generate traffic on target access point

Command Prompt

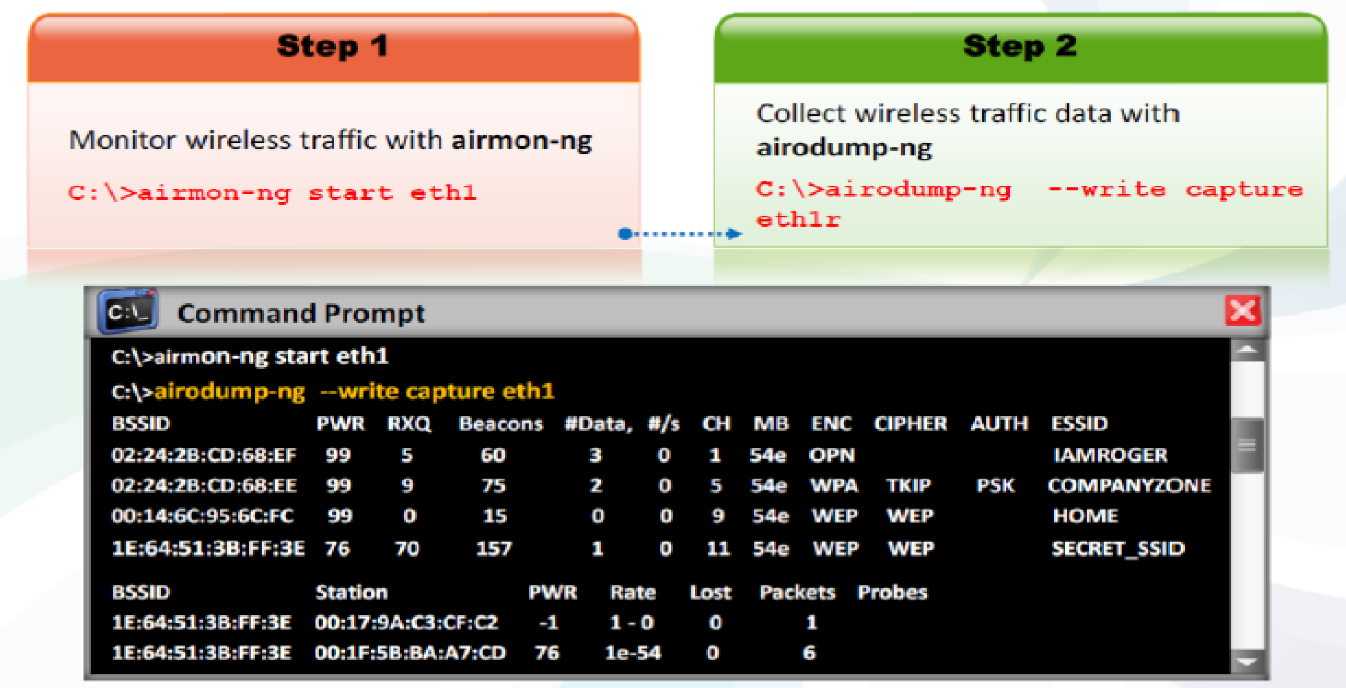
```
C:\>aircrack-ng -s capture.ivs
Opening capture.ivs
Read  75168 packets.
                          Aircrack-ng 0.7 r130
                 [00:00:10] Tested 77 keys (got 684002 IVs)
KB depth byte(vote)
0 0/ 1 AE( 199) 29( 27) 2D( 13) 7C( 12) FE( 12) FF( 6) 39( 5) 2C( 3) 00( 0) 08( 0)
1 0/ 3 66( 41) F1( 33) 4C( 23) 00( 19) 9F( 19) C7( 18) 64( 9) 7A( 9) 7B( 9) F6( 9)
2 0/ 2 5C( 89) 52( 60) E3( 22) 10( 20) F3( 18) 8B( 15) 8E( 15) 14( 13) D2( 11) 47( 10)
3 0/ 1 FD( 375) 81( 40) 1D( 26) 99( 26) D2( 23) 33( 20) 2C( 19) 05( 17) 0B( 17) 35( 17)
              KEY FOUND! [ AE:66:5C:FD:24 ]
```

Step 5: Wait for airodump-ng to capture more than 50,000 IVs Crack WEP key using aircrack-ng.

كيف كسر تشفير WPA-PSK باستخدام Aircrack

WPA-PSK هو أليه مصادقة التي توفر للمستخدمين نموذج بيانات الاعتماد لمصادقة شبكة. آليات التشفير المستخدمة في **WPA** و**WPA-PSK** هي نفسها، ولكن الفرق الوحيد بين هذين هو المصادقة إلى كلمة مرور حيث تم تخفيضها كلمة مرور بسيطة وشائعه في **WPA-PSK**. والمفتاح المشترك (**PSK**) في **WPA** عرضه لنفس المخاطر كأي نظام كلمة مرور مشترك أخر. **WPA-PSK** يمكن كسره باستخدام أداة **Aircrack**. فيما يلي الخطوات لكسر **WPA** مع **Aircrack**:

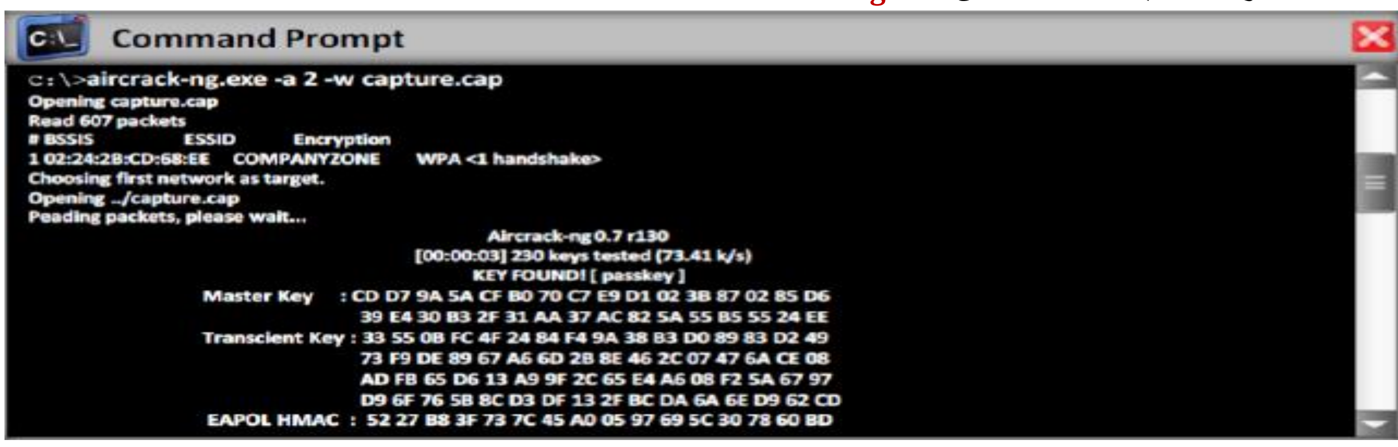
- الخطوة 1: رصد حركة المرور اللاسلكية مع **airmon-ng**.
- الخطوة 2: جمع بيانات حركة المرور اللاسلكية مع **airodump-ng**.



- الخطوة 3: إزالة (**deauth**) مصادقة العميل باستخدام **Aireplay-ng**. سيقوم العميل بمحاولة المصادقة مع **AP**، والتي سوف تؤدي إلى قيام **Airodump-ng** الى التقاط حزمة مصادقة **WPA** (المصافحة).



- الخطوة 4: تشغيل ملف الالتقاط من خلال **Aircrack-ng**.



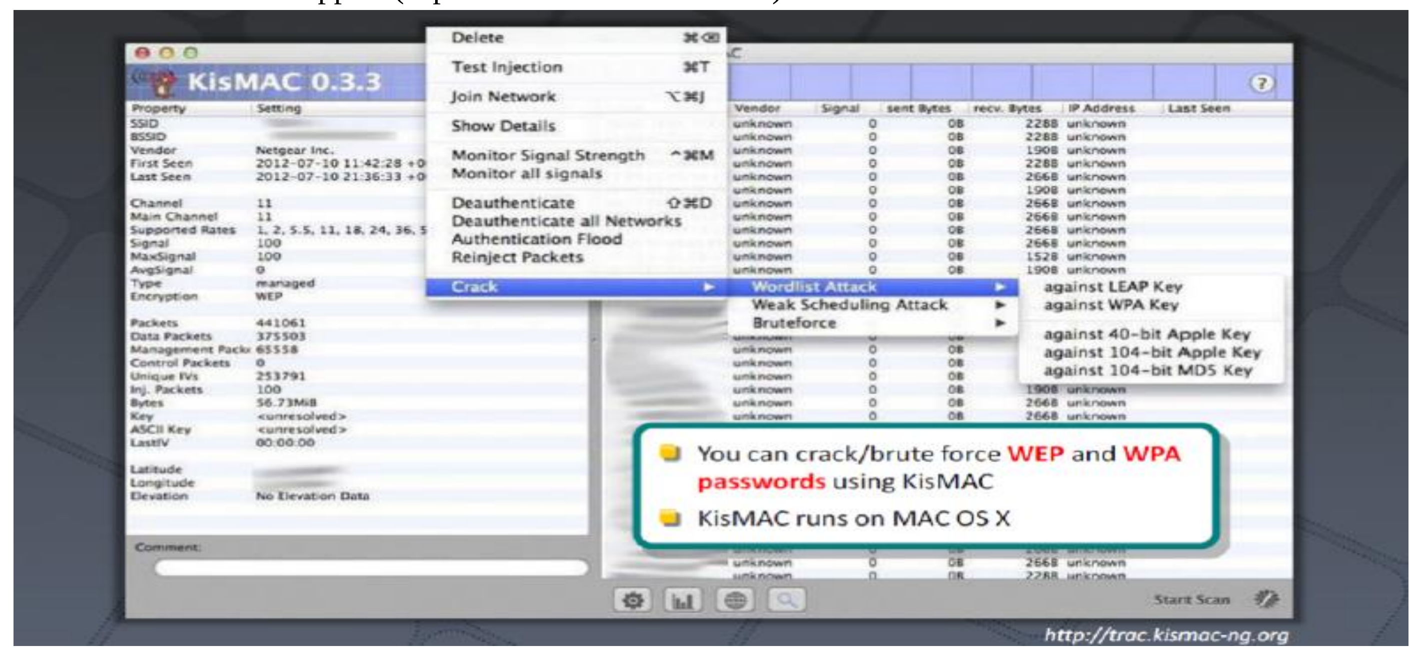
WPA Cracking Tool: KisMAC

المصدر: https://kismac-ng.org

KisMAC هو تطبيق للتنصت/فحص لنظام التشغيل **Mac OS X**. فإنه يستخدم وضع المراقبة و**passive scanning**. وهو يدعم العديد من أجهزة **USB** الخارجية مثل **Intersil Prism2**، **Ralin rt2570**، **rt73**، ورقائق **Realtek rtl8187**. كافة أجهزة AirPort الداخلية معتمده في الفحص.

عدد قليل من السمات التي تشملها KisMAC كالاتي:

- Reveals hidden / cloaked / closed SSIDs
- Shows logged in clients (with MAC addresses, IP addresses, and signal strengths)
- Mapping and GPS support
- Can draw area maps of network coverage
- PCAP import and export
- Support for 802.11b/g
- Different attacks against encrypted networks
- Deauthentication attacks
- AppleScript-able
- Kismet drone support (capture from a Kismet drone)



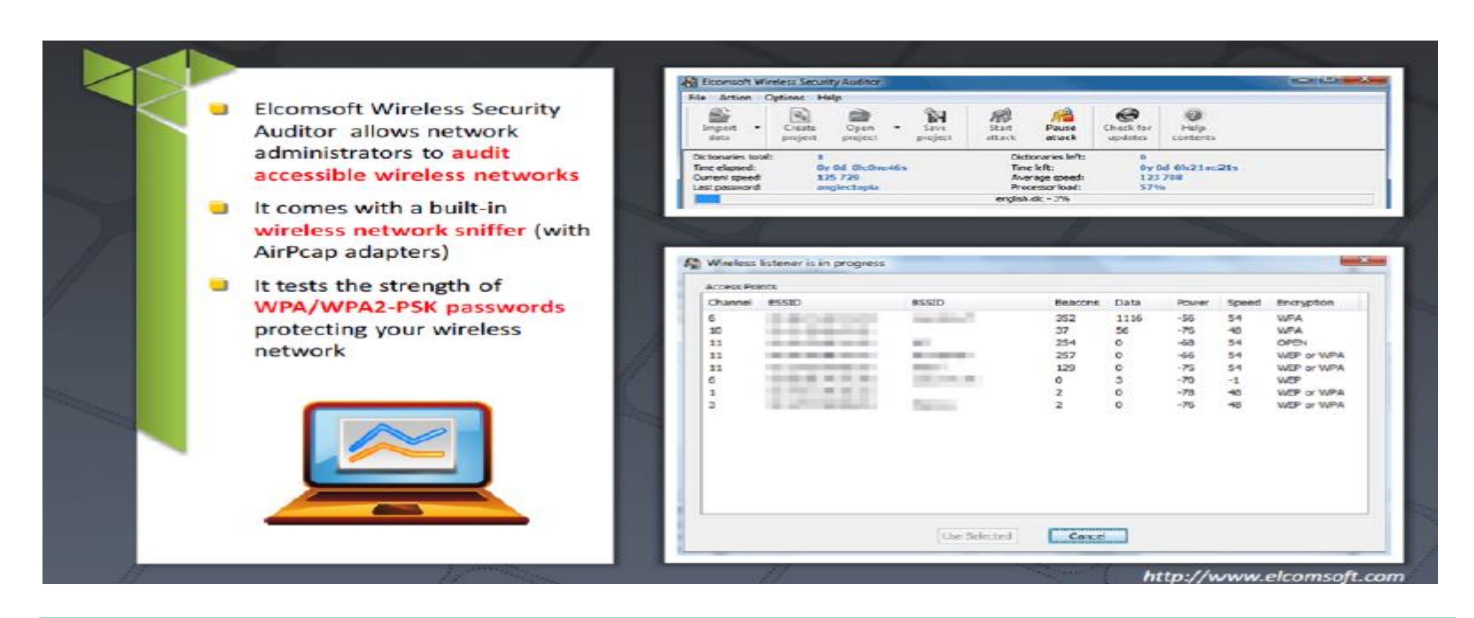
WEP Cracking Using Cain & Abel

Cain & Abel هي أداة لاستعادة كلمة السر لأنظمة التشغيل **Microsoft**. أداة كسر **WEP** في **Cain & Abel** تنفذ الكسر وطريقة **PTW cracking** لاسترداد مفتاح **WEP**. تسمح هذه الأداة باستعادة الأنواع المختلفة من كلمات المرور من خلال التنصت على الشبكة، كسر كلمات السر المشفرة باستخدام هجمات القاموس و**brute force** وتحليل الشفرات، تسجيل محادثات **VoIP**، فك كلمات المرور المشفرة، استعادة مفاتيح الشبكة اللاسلكية، كشف كلمة المرور، الكشف عن كلمات المرور المخزنة مؤقتاً، وتحليل بروتوكولات التوجيه. أحدث إصدار يتضمن ميزة جديدة، **APR (ARP Poison Routing)**، الذي يتيح التنصت على **switched LANs** وهجمات رجل في الوسط. التنصت في هذا الإصدار يمكن أيضا تحليل البروتوكولات المشفرة مثل **SSH-1** و**HTTPS**، ويحتوي على مرشحات لفلترة بيانات الاعتماد من طائفة واسعة من آليات المصادقة.

WPA Cracking Tool: Elcomsoft Wireless Security Auditor

المصدر: https://www.elcomsoft.com

Elcomsoft Wireless Security Auditor يسمح لك بالتحقق من أمان الشبكة اللاسلكية للشركة بتنفيذ مجموعه من التحقيقات الأمنية للشبكات اللاسلكية الموجودة. يأتي مع اداه للتنصت على شبكة اتصال لاسلكية مدمجة (مع محولات **AirPcap**). أنها تحاول استرداد كلمات المرور **WPA/WPA2-PSK** ذات النص الواضح من أجل اختبار كيفية تأمين البيئة اللاسلكية الخاصة بك.



WEP/WPA Cracking Tools

تستخدم أدوات كسر **WEP/WPA** لكسر المفاتيح السرية **WEP 802.11**. هذه الأدوات تقوم باسترداد مفتاح **WEP** من **40 بت** أو **104 بت**، **256 بت**، أو **512 بت** بمجرد التقاط ما يكفي من حزم البيانات. عدد قليل من الأدوات تقوم بتخمين مفاتيح **WEP** استناداً على هجوم **dictionary** النشط، مولد المفتاح، الهجوم على الشبكة الموزعة، إلخ. وفيما يلي عدد قليل من أدوات كسر **WEP/WPA** المستخدمة من قبل المهاجمين:

WepAttack available at http://wepattack.sourceforge.net
Wesside-ng available at http://www.aircrack-ng.org
Aircrack-ng available at http://www.aircrack-ng.org
WEPCrack available at http://wepcrack.sourceforge.net
WepDecrypt available at http://wepdecrypt.sourceforge.net
Portable Penetrator available at http://www.secpoint.com
CloudCracker available at http://www.cloudcracker.com
Wifite available at http://code.google.com
WepOff available at http://www.ptsecurity.ru

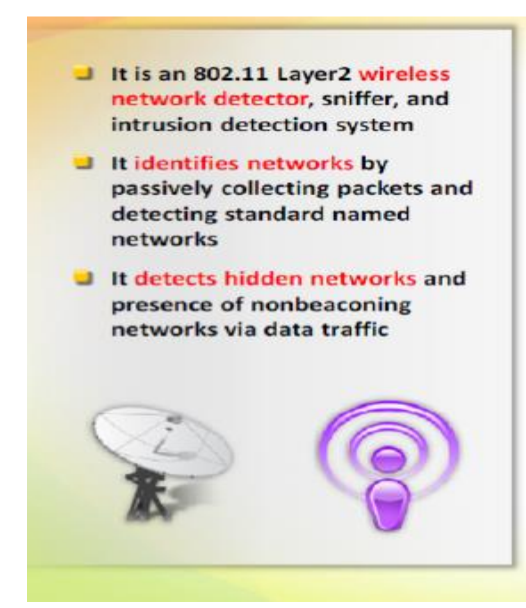
15.5 ادوات قرصنة الشبكات اللاسلكية "Wireless Hacking Tools"

حتى الآن، قد ناقشنا مختلف المفاهيم اللاسلكية والتشفير اللاسلكي، والتهديدات، ومنهجية القرصنة. الآن سوف نناقش أدوات قرصنة الشبكة اللاسلكية. يمكن أيضا إجراء القرصنة اللاسلكية مع مساعدة من الأدوات. أدوات القرصنة اللاسلكية تسهل مهمة المهاجم. يغطي هذا القسم مختلف أدوات التنصت اللاسلكي، وأدوات **wardriving**، أدوات رصد الترددات اللاسلكية، وتحليل حركة مرور الواي فاي، إلخ.

WI-FI SNIFFER: KISMET

المصدر: http://www.kismetwireless.net

Kismet هو **802.11 layer2 wireless network detector**، **sniffer**، ونظام لكشف التسلل. **Kismet** يعمل مع أي بطاقة لاسلكية تدعم الوضع **raw monitoring** (**rfmon**) ، ويمكنه التنصت على حركة المرور 802.11a، 802.11b، 802.11n، و802.11g (الأجهزة وبرامج التشغيل التي تسمح). وهو يحدد الشبكات من خلال جمع الحزم بصورة سلبية والكشف عن مستوى الشبكات، والكشف عن اسم الشبكة المخفية، واستنتاج وجود شبكات **non-beaconing** عن طريق بيانات حركة المرور.





WARDRIVING TOOLS

أدوات **Wardriving** تمكن المستخدمين من سرد قائمه بجميع نقاط الوصول التي تبث إشارات **beacon** في موقعهم. وهو يساعد المستخدمين على انشاء مجموعة جديدة من نقاط الوصول، مع التأكد من أنه ليس هناك نقاط **AP** متداخله. هذه الأدوات تتحقق من إعداد شبكة الاتصال، والعثور على المواقع مع ضعف التغطية في الشبكات اللاسلكية، وكشف الشبكات الأخرى التي قد تسبب التدخل. الكشف عن نقاط الوصول الغير مصرح بها **rouge** في الأدوات الخاصة بك في مكان العمل:

airbase-ng available at http://aircrack-ng.org
ApSniff available at http://www.monolith81.de
WiFiFoFum available at http://www.aspecto-software.com
MiniStumbler available at h http://www.netstumbler.com
WarLinux available at http://sourceforge.net
MacStumbler available at http://www.macstumbler.com
WiFi-Where available at http://www.threejacks.com
AirFart available at http://airtraf.sourceforge.net
AirTraf available at http://airtraf.sourceforge.net
802.11 Network Discovery Tools available at http://wavelan-tools.sourceforge.net

RF MONITORING TOOLS

أدوات رصد ترددات الراديو (**RF**) تساعد في اكتشاف ورصد شبكات **Wi-fi**. تساعدك هذه الأدوات لمراقبة ورصد واجهات شبكة الاتصال، بما في ذلك تلك اللاسلكية. أنها تسمح لك بالاطلاع على نشاط الشبكة وتساعدك على التحكم في واجهات الشبكة بطريقة مريحة. وفيما يلي قائمة بأدوات مراقبة الترددات اللاسلكية:

KWiFiManager available at http://kwifimanager.sourceforge.net
NetworkControl available at http://www.arachnoid.com
KOrinoco available at http://korinoco.sourceforge.net/
Sentry Edge II available at http://www.tek.com
WaveNode available at http://www.wavenode.com



xosview available at http://xosview.sourceforge.net
RF Monitor available at http://www.newsteo.com
OTC-340 RFXpert available at http://www.dektec.com
Home Curfew RF Monitoring System available at http://solutions.3m.com

WI-FI TRAFFIC ANALYZER TOOLS

أدوات تحليل حركة المرور اللاسلكية المرور تقوم بتحليل وتصحيح، والحفاظ على ورصد اتصالات الإنترنت من اجل الأداء، واستخدام عرض النطاق الترددي، وقضايا الأمن والشبكات المحلية. تقوم بالتقاط البيانات التي تمر عبر بطاقة إيثرنت الشبكة أو الاتصال الهاتفي، وتحليل هذه البيانات، ومن ثم تمثيلها في شكل يمكن قراءته بسهولة. هذا النوع من الادوات مفيدة للمستخدمين الذين يحتاجون إلى صورة شاملة لحركة المرور من خلال شبكة الاتصال أو قطعة من شبكة الاتصال المحلية. يقوم بتحليل حركة مرور الشبكة لتتبع المعاملات الخاصة أو البحث عن الخروقات الأمنية:

RFProtect Spectrum Analyzer available at http://www.arubanetworks.com
AirMagnet WiFi Analyzer available at http://www.flukenetworks.com
OptiView® XG Network Analysis Tablet available at http://www.flukenetworks.com
Observer available at http://www.netinst.com
Ufasoft Snif available at http://www.ufasoft.com
vxSniffer available at http://www.cambridgevx.com
OneTouch™ AT Network Assistant available at http://www.flukenetworks.com
Capsa Network Analyzer available at http://www.colasoft.com
SoftPerfect Network Protocol Analyzer available at http://www.softperfect.com

WI-FI RAW PACKET CAPTURING AND SPECTRUM ANALYZING TOOLS

❖ Raw Packet Capturing Tools

أدوات التقاط حزم **raw** تلتقط حزم الشبكة اللاسلكية، وتساعدك في رصد أنشطة **WLAN**. هذه الأدوات من اجل التقاط الحزم اللاسلكية لكل حزمة في الهواء ودعم **Ethernet LAN** و**802.11** وعرض حركة مرور شبكة الاتصال على مستوى **MAC**. يتم سرد عدد قليل من هذه الأنواع من الأدوات كما يلي:

WirelessNetView available at http://www.nirsoft.net
Tcpdump available at http://www.tcpdump.org
Airview available at http://airview.sourceforge.net
RawCap available at http://www.netresec.com
Airodump-ng available at http://www.aircrack-ng.org

❖ Spectrum Analyzing Tools

أدوات تحليل الطيف مصممة خصيصا لتحليل طيف الترددات اللاسلكية واستكشاف الأخطاء وإصلاحها. مع المساعدة من هذه الأدوات، فان المستخدمين يمكنهم الكشف عن أي نشاط في بيئة الترددات اللاسلكية، بما في ذلك الكشف عن المناطق التي تؤثر على الترددات اللاسلكية وتدخل في الأداء والتي تؤدى في نهاية المطاف إلى استياء المستخدم بسبب بطء الاتصال أو الانقطاع المتكرر. مع هذه المعلومات، يمكن للمستخدمين تحديد قنوات أفضل لنشر نقاط اتصال الواي فاي:

Cisco Spectrum Expert available at http://www.cisco.com
AirMedic USB available at http://www.flukenetworks.com
AirSleuth-Pro available at http://nutsaboutnets.com
BumbleBee-LX Handheld Spectrum Analyzer available at http://www.bvsystems.com
Wi-Spy available at http://www.metageek.net

15.6 قرصنة البلوتوث "Bluetooth Hacking"

البلوتوث هي خدمة لاسلكي تسمح بمشاركة الملفات. قرصنة البلوتوث يسمح للمهاجم بالحصول على معلومات المضيف من جهاز بلوتوث آخر دون إذن المضيف. مع هذا النوع من القرصنة، فان المهاجم يمكنه سرقة المعلومات وحذف جهات الاتصال من الهواتف النقالة الضحية واستخراج الملفات/الصور الشخصية، إلخ. يتم شرح أنواع مختلفة من هجمات البلوتوث والأدوات التي يتم استخدامها للقيام بمثل هذه الهجمات في الشرائح التالية.

البلوتوث هي تكنولوجيا اتصالات لاسلكية قصيرة المدى تهدف إلى استبدال الكابلات التي تستخدم في توصيل الأجهزة المحمولة أو الثابتة مع الحفاظ على مستويات عالية من الأمن. انه يسمح للهواتف النقالة وأجهزة الكمبيوتر والأجهزة الأخرى بتبادل المعلومات باستخدام اتصال لاسلكي قصير المدى. اثنين من الأجهزة ذات اتصال بلوتوث تتصلا مع بعض عن طريق تقنية **pairing**. هناك بعض القضايا الأمنية المتعلقة بالبلوتوث مما يجعل من الممكن اختراق البلوتوث وجعل عملية اختطاف جلسات البلوتوث بين الأجهزة ممكنة. قرصنة البلوتوث يشير إلى استغلال نقاط الضعف في البلوتوث والتي ينتج عنها اختراق البيانات الحساسة في الأجهزة والشبكات الداعمة للبلوتوث. فيما يلي بعض أنواع الهجمات على جهاز البلوتوث:

- **Bluejacking**

Bluejacking يستخدم البلوتوث لإرسال رسائل إلى المستخدمين من دون موافقه المستلم، مماثلة لـ **email spamming**. قبل أي اتصال بلوتوث، الجهاز المنشئ للاتصال لابد من توفير اسم سيتم عرضه على شاشة المستلم. لأن هذا الاسم تعريف المستخدم، يمكن ضبطه ليكون رسالة أو إعلان مزعج. على وجه التحديد، **Bluejacking** لا يسبب أي ضرر لجهاز الاستقبال. ومع ذلك، يمكن ان يكون مزعج ومدمر لضحاياه.

- **BlueSniff**

BlueSniff هو قائم على اساس التعليمات البرمجية لأداة **Bluetooth wardriving**. أنها مفيدة للعثور على أجهزة البلوتوث المخفية وقابل للاكتشاف. وهو يعمل على لينكس.

- **Bluesmacking**

هجوم **Bluesmacking** يحدث عندما يرسل المهاجم حزمة **ping** متضخمة إلى جهاز الضحية. يؤدي هذا الى تجاوز سعة المخزن المؤقت في جهاز الضحية. يشبه هذا النوع من الهجوم هجوم **ICMP ping of death**.

- **Bluesnarfing**

Bluesnarfing هو أسلوب الوصول إلى البيانات الحساسة في جهاز البلوتوث. إذا كان مهاجم ضمن نطاق الهدف، فانه يمكن استخدام البرمجيات الخاصة للحصول على البيانات المخزنة على جهاز الضحية. للقيام بهذا النوع من الهجوم، فان مهاجم يستغل مشكلة في البروتوكول الذي يستخدمه البلوتوث لتبادل المعلومات. ويسمى هذا البروتوكول **Object Exchange (OBEX)**. المهاجم يرتبط مع الهدف وينفذ عملية الحصول على الملفات ذات الأسماء المعروفة أو خمنت بشكل صحيح، مثل **/pb.vcf**، المخصص لدفتر الهاتف أو الاتصالات، الملف **/cal.vcs** لملف التقويم للجهاز.

مكدس البلوتوث (BLUETOOTH STACK)

مكدس البلوتوث يشير إلى تطبيق مكدس بروتوكول البلوتوث. أنه يسمح للتطبيق المورث بالعمل عبر تقنية البلوتوث. يتم استخدام الموديل **Atinav's OS abstraction layer**، لإنشاء المنفذ الى البلوتوث. وينقسم مكدس البلوتوث الى: **general purpose** و **embedded system**.

أوضاع البلوتوث (Bluetooth mode)

- **الوضع القابل للاكتشاف (Discoverable Mode)**

أساسا، البلوتوث يعمل في ثلاثة أنماط قابلة للاكتشاف. وهم:

Discoverable: عندما تكون أجهزة البلوتوث في الوضع **discoverable mode**، فان الأجهزة ترى من خلال أجهزة البلوتوث الأخرى. إذا كان الهاتف يحاول الاتصال بهاتف آخر، فان الهاتف الذي يحاول تأسيس الاتصال يجب أن يبحث عن هاتف موجود في "الوضع

discoverable mode، خلاف ذلك سيكون الهاتف غير قادراً على الكشف عن الهاتف الآخر. **Discoverable mode** ضروري فقط أثناء الاتصال بالجهاز لأول مرة. بمجرد حفظ الاتصال، فان الهواتف يعرفون بعضهم البعض؛ ولذلك، الوضع **Discoverable** يصبح غير ضروري.

Limited discoverable: في هذا الوضع، فان أجهزة البلوتوث تكون قابله للاكتشاف فقط لفترة محدودة من الزمن، لحدث معين، أو أثناء ظروف مؤقتة. ومع ذلك، لا يوجد أي أمر **HCI** لتعيين الجهاز مباشرة في الوضع **Limited discoverable**. يجب أن يكون ذلك غير مباشر. عندما يتم تعيين الجهاز إلى وضع الاكتشاف المحدود، فانه يقوم بتصفية **IACs** الغير مطابقة ويكتشف بنفسه تلك التي تطابق.

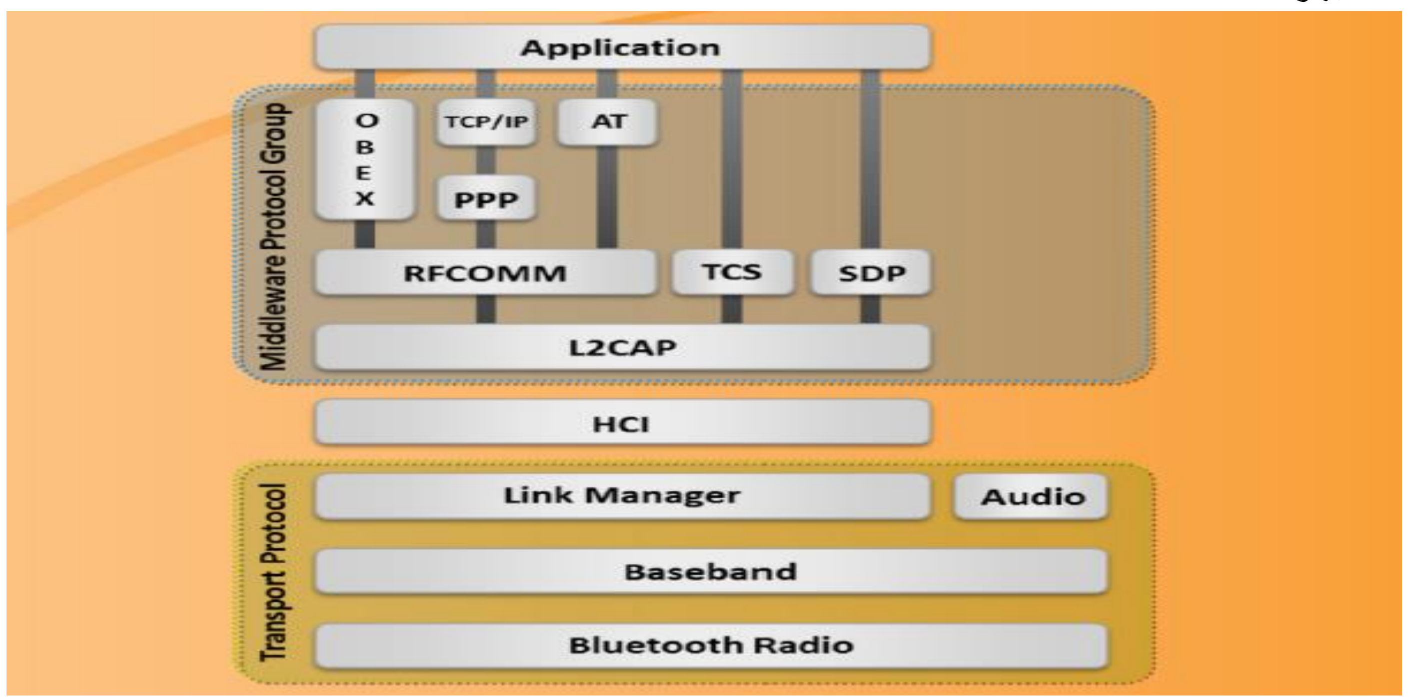
Non-discoverable: إعداد جهاز البلوتوث إلى هذا الوضع يمنع ظهور الأجهزة في القائمة الناتجة خلال عملية البحث عن جهاز بلوتوث. ومع ذلك، فأنها لا تزال مرئية لهؤلاء المستخدمين والأجهزة الذين اقترنا جهاز البلوتوث لديهم بهذا الجهاز سابقا أو على دراية بعنوان **MAC** البلوتوث.

- **الوضع Pairing mode**

هناك اثنين من **Pairing mode** لأجهزة البلوتوث. وهم:

Non-pairable mode: في هذا الوضع، فان جهاز البلوتوث يرفض طلب الإقران (**pairing**) المرسل من أي جهاز.

Pairable mode: في هذا الوضع، فان جهاز البلوتوث يوافق على طلب الإقران (**pairing**) المرسل من أي جهاز وتأسيس اتصال مع هذا الجهاز.



BLUETOOTH THREATS

مثل الشبكات اللاسلكية، فان أجهزة البلوتوث تخضع أيضا الى العديد من التهديدات. بسبب الثغرات الأمنية في تقنية البلوتوث، فمن الممكن ان يحدث العديد من التهديدات الأمنية الخاصة بالبلوتوث. فيما يلي المخاطر التي تتهدد أجهزة البلوتوث:

- **تسرب التقويمات ودفاتر العناوين**: المهاجم يمكنه سرقة المعلومات الشخصية للمستخدم، ويمكنه استخدامها لأغراض خبيثة.
- **Bugging devices**: المهاجم يمكنه إرشاد المستخدم لإجراء مكالمة هاتفية إلى الهواتف الأخرى دون أي تفاعل من المستخدم. حتى أنها يمكن أن يسجل المحادثة للمستخدم.
- **إرسال رسائل SMS**: الإرهابيين يمكنهم إرسال تهديدات بوجود قنبلة مزيفه لشركات الطيران على سبيل المثال باستخدام هواتف المستخدمين الشرعيين.
- **التسبب في خسائر مالية**: القراصنة يمكنهم إرسال العديد من رسائل **MMS** مع هاتف المستخدم الدولي، والتي يسفر عن فاتورة هاتف مرتفعة.
- جهاز التحكم عن بعد: القراصنة يمكنهم التحكم عن بعد بالهاتف لإجراء مكالمات هاتفية أو الاتصال بالأنترنت.

- الهندسة الاجتماعية: المهاجمون يمكنهم خداع مستخدمي البلوتوث لخفض التدابير الأمنية أو تعطيل المصادقة في اتصال البلوتوث وذلك من اجل التشابك معه وسرقة المعلومات.
- الأكواد الضارة: **mobile phone worms** يمكن اختراق اتصال بلوتوث من اجل التكرار والانتشار.
- ضعف البروتوكول: المهاجمين يمكنهم اختراق **Bluetooth paring** وبروتوكولات الاتصال من اجل سرقة البيانات، إجراء المكالمات، إرسال الرسائل، وشن هجمات دوس على جهاز، بدء تشغيل الهاتف للتجسس، إلخ.

HOW TO BLUEJACK A VICTIM

Bluejacking هو 'الاختطاف المؤقت للهاتف الخليوي الخاص بشخص آخر عن طريق إرساله رسالة نصية أنانونيموس باستخدام نظام الشبكات اللاسلكية بلوتوث'. مدى شبكة البلوتوث هو 10 أمتار. الهواتف المزودة بتقنية البلوتوث يمكنها البحث عن الهواتف الاخرى المزودة بتقنية البلوتوث عن طريق إرسال رسائل إليهم. **Bluejacking** هو مصطلح جديد لتعريف نشاط إرسال رسائل مجهولة للأجهزة الأخرى المزودة بتقنية البلوتوث عن طريق البروتوكول **OBEX**. اتبع الخطوات المذكورة التالية من اجل **Bluejacking** الضحية او الأجهزة:

الخطوة الأولى: تحديد منطقة ملغومه بمستخدمي الهواتف المتحركة، مثل المقهى ومركز للتسوق، إلخ. انتقل سجل الاتصال (**contact**) الخاص بك.

الخطوة الثانية: إنشاء جهة اتصال جديدة في دفتر عناوين الهاتف الخاص بك. أدخل رسالة في حقل الاسم على سبيل المثال " **Would you like to go on a date with me**" (يمكنك حذف إدخال جهة الاتصال هذه في وقت لاحق).

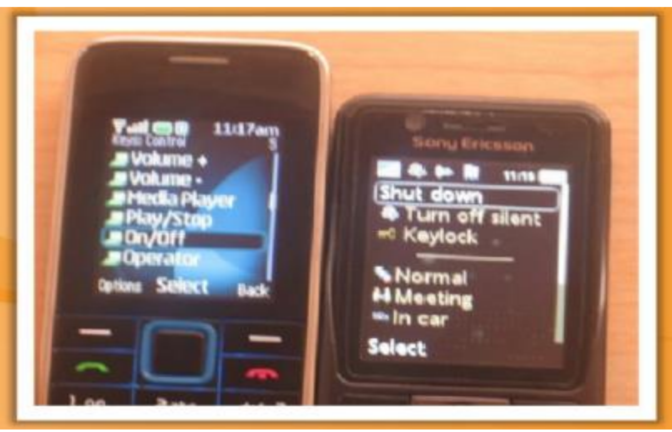
الخطوة الثالثة: حفظ جهة الاتصال الجديدة مع نص الاسم من دون رقم الهاتف. ومن ثم اختيار **send via Bluetooth**. وهذا يقوم بالبحث عن أي جهاز بلوتوث خلال النطاق.

الخطوة الرابعة: اختر هاتف واحد من قائمة اكتشاف البلوتوث ومن ثم اختيار **send the contact**. سوف تحصل على الرسالة " **card sent**" ومن ثم الاستماع لنغمة رسالة **SMS** من الهاتف الخاص بالضحية.

BLUETOOTH HACKING TOOL: SUPER BLUETOOTH HACK

بلوتوث تروجان، عند إصابته الهدف، فانه يسمح للمهاجم بالتحكم وقراءة المعلومات من هاتف الضحية. فإنه يستخدم أوامر **AT** البلوتوث للوصول او قرصنة أجهزة الهواتف الأخرى المدعمة لتقنية البلوتوث. بمجرد إصابة، تمكن المهاجمين من قراءة الرسائل والاتصالات وتغيير الشخصية والتلاعب بالنغمات، إعادة تشغيل أو إيقاف تشغيل الهاتف، استعادة إعدادات المصنع وإجراء مكالمات من الهاتف للضحية. **Super Bluetooth Hack** هو اداه لقرصنة أجهزة المحمول من خلال تقنية البلوتوث. تتطلب الأداة قبول الضحية اتصال بلوتوث أولاً، ولكن هذا إجراء مرة واحدة فقط لاقتران الهواتف. ثم أنها لا تتطلب المقارنة مرة اخرى.



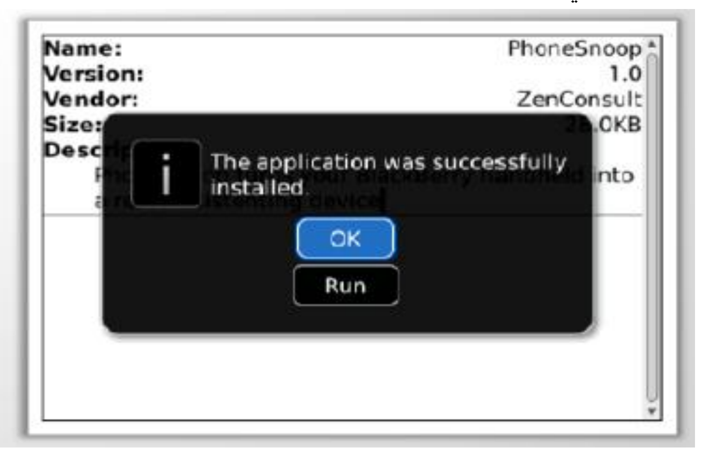


BLUETOOTH HACKING TOOL: PHONESNOOP

PhoneSnoop هو برنامج تجسس خاص بالبلاك بيري التي تمكن المهاجم عن بعد من تفعيل الميكروفون الخاص بالبلاك بيري المحمول والاستماع إلى الأصوات القريبة أو التي حوله؛ **PhoneSnoop** ناتج من بعض الخلل، والتي تثبيت مفهوم التجسس. أنه موجود فقط لإثبات

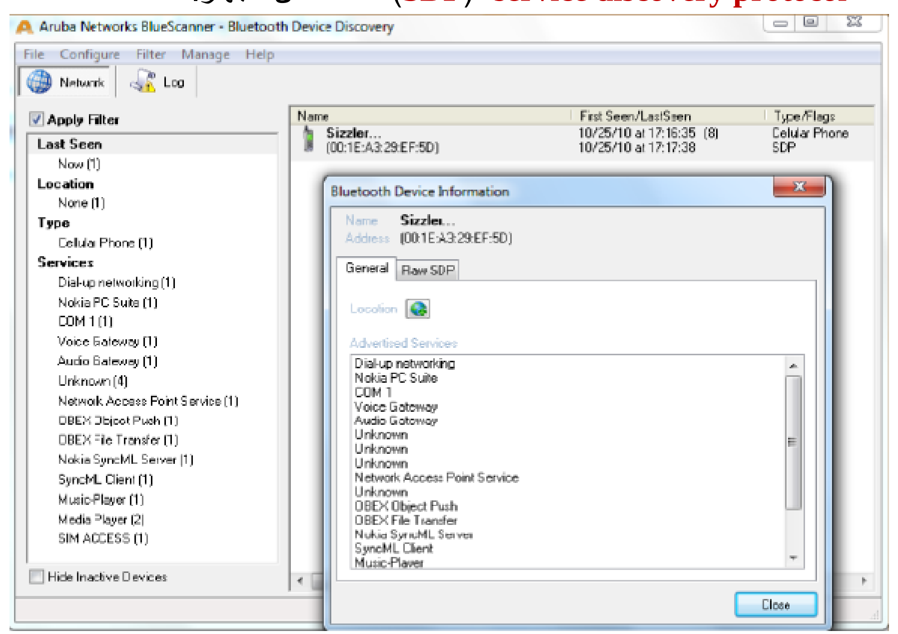
قدرات البلاك عندما يتم استخدامه لإجراء المراقبة على أساس فردي. هو محض تطبيق للإثبات ولا يمتلك أي من ميزات الشبح أو برامج التجسس التي تجعله خبيث.





BLUETOOTH HACKING TOOL: BLUESCANNER

BlueScanner هو أداة لاكتشاف أجهزة البلوتوث وتقييم لنقاط الضعف لنظام التشغيل **Windows XP**.
Aruba Networks BlueScanner يتم توفيره بموجب الترخيص **Aruba Software License**. مع محول بلوتوث، يمكن للمؤسسات استخدام **BlueScanner** لاكتشاف أجهزة البلوتوث، النوع (الهاتف، الكمبيوتر، لوحة المفاتيح، **PDA**، إلخ)، والخدمات التي يتم الإعلان عنها بالأجهزة. وسيكون تحديد أي أجهزة قابلة للاكتشاف ضمن النطاق وتسجيل جميع المعلومات التي يمكن جمعها من الجهاز، دون محاولة المصادقة مع الجهاز البعيد. تتضمن هذه المعلومات اسم الجهاز وعنوانه الفريد، النوع، وقت الاكتشاف، شوهد آخر مرة وأي بروتوكول اكتشاف الخدمات "**service discovery protocol**" (**SDP**) المقدمة من الجهاز.



BLUETOOTH HACKING TOOLS

أدوات قرصنة البلوتوث تسمح للمهاجمين لاستخراج قدر ممكن من المعلومات من جهاز البلوتوث من بدون الحاجة الى الاقتران. هذه الأدوات تستخدم لفحص الأجهزة أخرى التي تظهر من ضمن الناطق، ويمكن تنفيذ استعلام خدمة. يتم سرد عدد قليل من الأدوات المستخدمة لأداء قرصنة البلوتوث كما يلي:

BTBrowser available at http://www.bluejackingtools.com/java/bt-browser-20/
BH Bluejack available at http://croozeus.com



Bluesnarfer available at http://www.airdemon.net
BTCrawIer available at http://www.silentservices.de
Bluediving available at http://bluediving.sourceforge.net
Blooover available at http://trifinite.org
BTScanner available at http://www.pentest.co.uk
CIHwBT available at http://sourceforge.net
BT Audit available at http://trifinite.org
BlueAlert available at http://www.insecure.in

15.7 التدابير المضادة "counter measures"

حتى الآن، لقد ناقشنا مفاهيم الشبكات اللاسلكية، التشفير اللاسلكي، والتهديدات المرتبطة بالشبكات اللاسلكية، ومنهجية القرصنة، مختلف الأدوات لقرصنة الشبكة اللاسلكية، وقرصنة البلوتوث. كل هذه المفاهيم والأدوات تساعد في قرصنة أو اختراق الشبكة اللاسلكية. الآن سوف نذهب أكثر الى التدابير المضادة التي يمكن أن تساعد في تصحيح الثغرات الأمنية المحددة. التدابير المضادة هي ممارسة استخدام العديد من أنظمة الأمن أو التكنولوجيات لمنع الاختراقات. هذا القسم مخصص للتدابير المضادة، والممارسات التي تمكننا الدفاع بها ضد مختلف أساليب أو وسائل القرصنة.

HOW TO DEFEND AGAINST BLUETOOTH HACKING

على الرغم من أنه يجري سد الثغرات الأمنية دورياً حسب الشركة المصنعة والتقني، فيما يلي بعض النصائح التي ينبغي على المستخدم العادي الاعتبار بها، وحماية نفسه بعيداً عن الهاكر:

1- إبقاء البلوتوث في الحالة **disabled**؛ وتمكينه فقط عند الحاجة، وتعطيله فورا بعد إكمال المهمة المقصودة.
2- إبقاء الجهاز في الوضع **non-discoverable** (مخفي).
3- لا تقبل أي طلب إقران غير معروف وغير متوقع الى الجهاز الخاص بك.
4- الحفاظ على فحص كافة الأجهزة المقترنة في الماضي من وقت إلى وقت، وحذف أي جهاز غير متأكدة منه.
5- قم دائماً بتمكين التشفير عند إنشاء اتصال بلوتوث لجهاز الكمبيوتر الخاص بك.
6- استخدام الأنماط الغير عادية كمفاتيح **PIN** أثناء اقتران الجهاز. استخدم تركيبات المفاتيح هذه التي غير متتالية وغير واضحة على لوحة المفاتيح.

HOW TO DETECT AND BLOCK ROGUE APS

كشف وتجميد نقاط الوصول المزيفة هي المهام الهامة التي يتعين تنفيذها لضمان أمن الشبكة اللاسلكية وحماية الشبكة اللاسلكية من التعرض للاختراق.

الكشف عن نقاط وصول المارقة "Detecting Rouge APs"

نقاط الوصول المارقة هي واحده غير معتمدة من قبل مسؤول شبكة الاتصال للعملية. المشكلة المرتبطة بهذه **APs** المارقة أن هذه **APs** لا تتفق مع سياسات أمن الشبكات اللاسلكية. هذا يمكنه تمكين واجهة مفتوحة غير آمنة لشبكة الاتصال الموثوق بها. وهناك مختلف التقنيات المتاحة للكشف عن **AP** المارقة. فيما يلي تقنيات الكشف عن **AP** المارقة:

RF scanning: نقاط الوصول **Re-purposed** التي تفعل فقط التقاط الحزم والتحليل (أجهزة استشعار **RF**) تكون موصولة في جميع أنحاء الشبكة السلكية لكشف وتحذير مدير الشبكة المحلية اللاسلكية حول أي من الأجهزة اللاسلكية التي تعمل في المنطقة. أجهزة الاستشعار هذه لا تغطي **dead zones**. هذا يحتاج الى إضافة أجهزة استشعار أكثر، للكشف عن نقاط الوصول في المناطق الميتة.

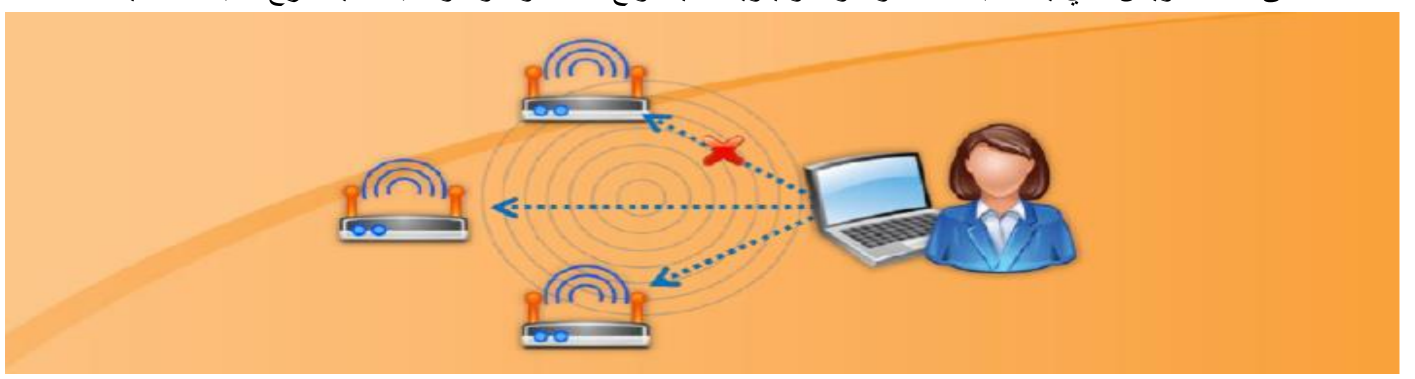
AP scanning: نقاط الوصول التي لديها الوظيفة للكشف عن نقاط الوصول المجاورة في المنطقة المجاورة سوف يعرض البيانات من خلال **MIBS** وواجهة ويب. في هذه الحالة **drawback** هي ان قدرة نقاط الوصول لاكتشاف الأجهزة المجاورة محدودة إلى حد ما.

Using wired side inputs: برامج إدارة شبكة الاتصال يستخدم هذه التقنية للكشف عن نقاط الوصول المارقة. هذا البرنامج يقوم بالكشف عن الأجهزة المتصلة بالشبكة المحلية، بما في ذلك **Telnet**، **SNMP**، و**CDP** (بروتوكول اكتشاف سيسكو) باستخدام بروتوكولات متعددة. بغض النظر عن مكان تواجدها، يمكن اكتشاف نقاط الوصول الموجودة في أي مكان في الشبكة باستخدام هذا الأسلوب.

حجب نقاط الوصول المارقة "Blocking Rouge AP"

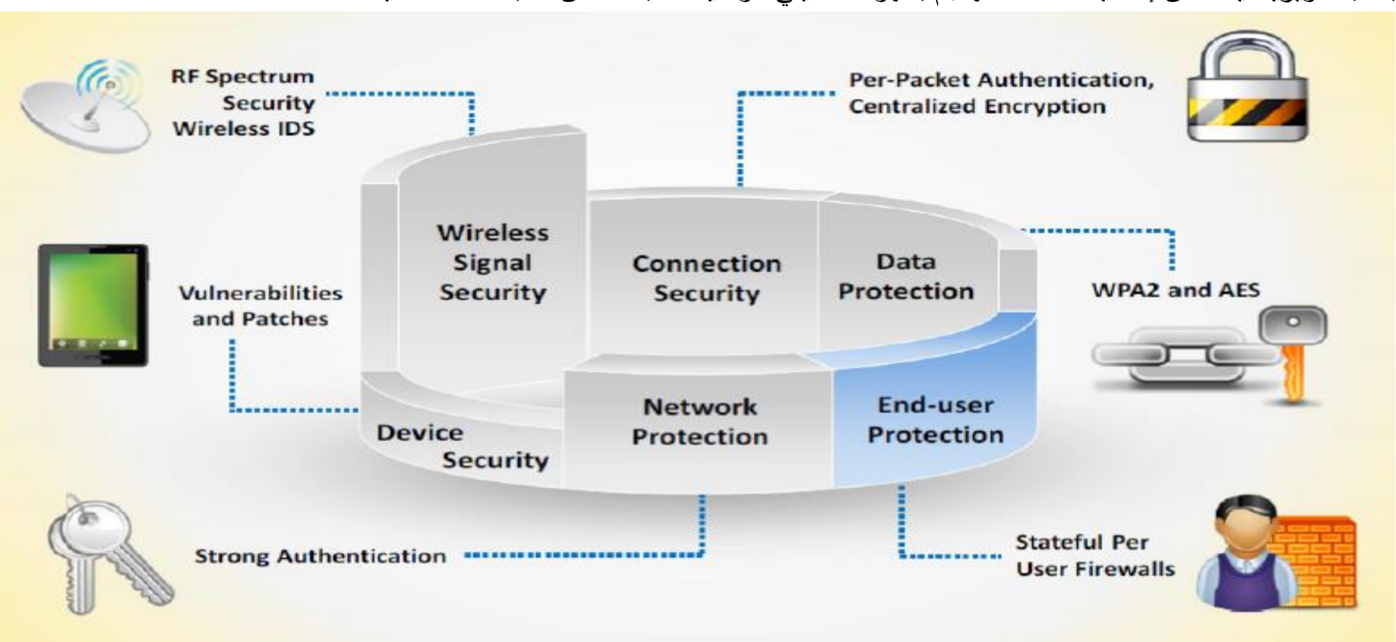
إذا كان هناك أي من نقاط الوصول المارقة في الشبكة اللاسلكية المحلية، فيجب ان يتم حظره فورا لتجنب ارتباط المستخدمين المخولين أو العملاء بها. يمكن أن يتم ذلك بطريقتين:

- رفض الخدمة اللاسلكية للعملاء الجدد بشن هجوم رفض الخدمة (**DoS**) على **Rouge AP**.
- غلق منفذ السويتش الذي يتصل به نقطة الوصول أو يدوياً تحديد موقع نقطة الوصول وسحبه فعلياً خارج الشبكة المحلية.



WIRELESS SECURITY LAYERS

أليه أمان الشبكة اللاسلكية يضم ست طبقات لضمان الأمن المتصلة بمختلف القضايا. هذه الطبقات تزيد من نطاق منع المهاجم من المساس بالشبكة ويزيد أيضا من إمكانية امساك المهاجم بسهولة. ما يلي هو هيكل طبقات أمن الشبكات اللاسلكية:



Connection security: في عملية المصادقة لكل إطار/حزمة يتم توفير حماية كاملة ضد هجمات رجل في المنتصف "**MITM**". أنه لا يسمح للمهاجم بالتنصت على البيانات عندما يتم توصيل اثنين من المستخدمين الحقيقيين بين بعضهما البعض وبالتالي تأمين الاتصال.

Device security: كل من ادارة نقاط الضعف والتصحيح هي مكون هام من البنية التحتية الأمنية، حيث ان هذان العنصران مهمان لكشف ومنع الثغرات الأمنية قبل أن يساء استخدامها فعلا والمساس بأمن الجهاز.

Wireless signal security: في الشبكات اللاسلكية، مواصلة رصد وإدارة الترددات اللاسلكية و**RF spectrum** داخل البيئة يحدد التهديدات وقدرات الوعي. نظام كشف التسلل اللاسلكية (**WIDS**) لديه القدرة على تحليل ورصد طيف الترددات اللاسلكية

RF spectrum. يمكن اكتشاف الأجهزة اللاسلكية الغير مأذون لها التي تنتهك السياسات الأمنية للشركة بتوليد إنذار. الأنشطة مثل استخدام زائد في عرض النطاق الترددي، **RF interferences**، ونقاط الوصول المارقة الغير معروفه وهكذا هي دلائل على الشبكة الضارة. مع المساعدة من هذه الدلائل يمكنك الكشف بسهولة عن الشبكة الخبيثة ويمكن الحفاظ على أمن الشبكات اللاسلكية. لا يمكن التنبؤ بالهجمات على شبكة الاتصال اللاسلكية. الرصد المستمر للشبكة هو المقياس الوحيد التي يمكن استخدامه لمنع مثل هذه الهجمات وتأمين شبكة الاتصال.

Network protection: المصادقة القوية تضمن فقط للمستخدم ذات الإذن الحصول على حق الوصول إلى شبكة الاتصال الخاصة بك وبالتالي حماية الشبكة الخاصة بك من المهاجمين.

Data protection: يمكن القيام بحماية البيانات من خلال تشفير هذه البيانات من خلال استخدام بعض لوغاريتمات التشفير مثل **WPA2** و**AES**.

End-user protection: حتى إن اصبح المهاجم مرتبط بنقطة الوصول، فان جدار الحماية الشخصي الموجودة في نظام المستخدم يمنع المهاجم من الوصول الى الملفات الموجودة في نظام المستخدم، وذلك فهي تحمى المستخدم.

كيفية الدفاع ضد الهجمات اللاسلكية

بجانب استخدام أدوات رصد أمن الشبكة اللاسلكية، فان المستخدمين يمكنهم اتباع بعض المنهجيات للدفاع عن شبكاتها ضد مختلف التهديدات والهجمات. وفيما يلي بعض أفضل الاعدادات المكونة للشبك اللاسلكية والتي تضمن أمن الشبكات اللاسلكية:

- تغيير **SSID** بعد تكوين الشبكات اللاسلكية.
- تعيين كلمة مرور الوصول إلى جهاز الراوتر وتمكين جدار الحماية.
- تعطيل بث **SSID**.
- تعطيل الوصول الى جهاز الراوتر وإدارة الشبكة اللاسلكية عن بعد.
- تمكين تصفية عناوين **MAC** في نقطة الوصول أو جهاز التوجيه الخاص بك.
- تمكين التشفير في نقطة الوصول، وتغيير كلمة المرور.

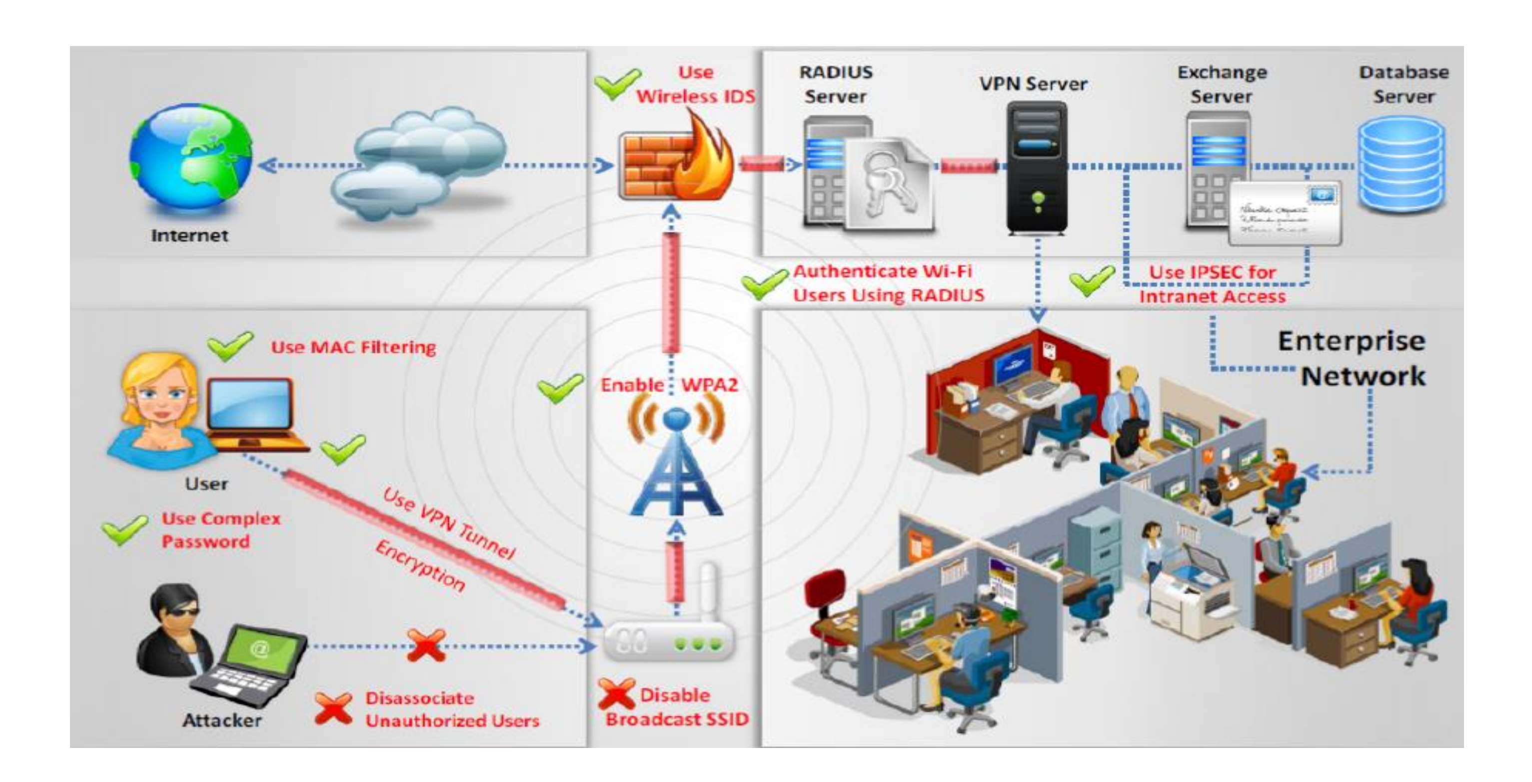
يمكن حماية الشبكات اللاسلكية من الهجمات اللاسلكية المختلفة عن طريق تغيير إعدادات **SSID** لتوفير أمن رفيع المستوى. وفيما يلي طرق لتعيين إعدادات **SSID** التي تضمن أمن الشبكات اللاسلكية:

- استخدام **SSID cloaking** لإبقاء بعض الرسائل اللاسلكية من بث **ID** للجميع.
- لا تستخدم **SSID** الخاص بك، اسم الشركة، اسم الشبكة، أو أي من يكون سهل تخمينه.
- ضع جدار حماية أو مفلتر الحزم ما بين نقطة الوصول وشبكة الانترنت.
- تحديد حدود قوة الشبكة اللاسلكية حيث أنه لا يمكن أن تكشف خارج حدود المؤسسة الخاصة بك.
- التحقق من الأجهزة اللاسلكية من اجل اكتشاف مشاكل التكوين أو الإعداد بانتظام.
- تنفيذ تقنية مختلفة لتشفير حركة المرور، مثل **IPSec over wireless**.

إعداد المصادقة القوية للوصول إلى شبكات الواي فاي يعتبر اجراء للدفاع عن الشبكة المحلية اللاسلكية ضد الهجمات اللاسلكية. وفيما يلي طرق لتعيين المصادقة لاسلكياً إلى مستوى أقوى:

- اختر الوصول المحمي اللاسلكي (**WPA**) بدلاً من **WEP**.
- تنفيذ مشاريع **WPA2 Enterprise** إن أمكن.
- تعطيل الشبكة عند عدم الحاجة اليها.
- وضع نقاط الوصول اللاسلكية في موقع مضمون.
- الحفاظ على جميع المعدات اللاسلكية محدثه.
- استخدام خادم مركزي للمصادقة.

اعتمدت العديد من تقنيات الدفاع للاسلكية حماية الشبكة ضد الهجمات اللاسلكية وقد ناقشناهم في وحدة سابقة. استخدام **WIDS** المناسبة، ملقم **RADIUS** وغيرها من الآليات الأمنية في المكان المناسب يمكنها الدفاع عن الشبكة اللاسلكية الخاصة بك من التعرض للهجوم.

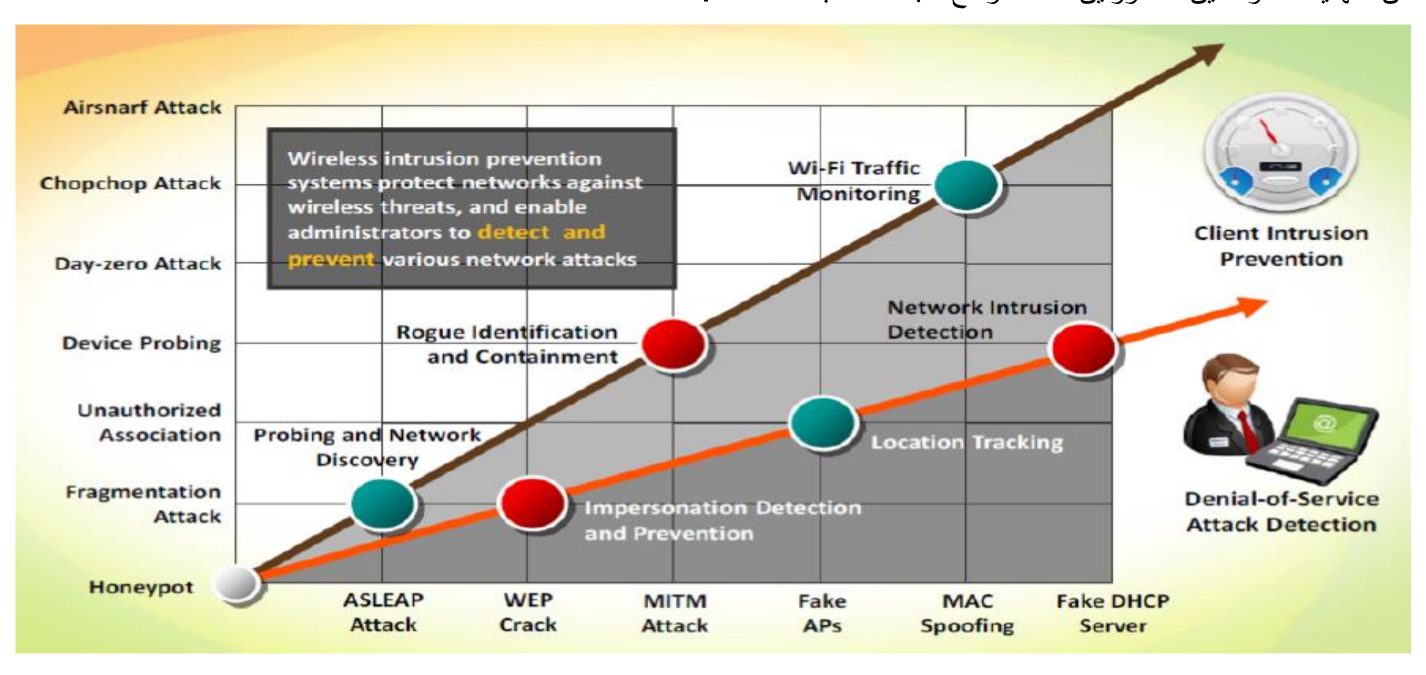


15.8 أدوات أمن الشبكات اللاسلكية "Wireless security tools"

يمكن تحقيق أمن الشبكات اللاسلكية ليس فقط بالأساليب اليدوية ولكن أيضا مع أدوات الأمان اللاسلكي. استخدام أدوات الأمن بجانب الأساليب اليدوية يجعل الشبكات اللاسلكية أكثر أماناً. هذا القسم مخصص لآليات وأدوات الأمان اللاسلكي.

Wireless Intrusion Prevention Systems

نظام منع التسلل لاسلكية (**WIPS**) هو جهاز شبكي لرصد طيف الراديو للكشف عن نقاط الوصول (كشف التسلل) دون الحصول على إذن المضيفين في مواقع قريبة، ويمكن أيضا تطبيق التدابير المضادة تلقائياً. أنظمة منع الاختراق اللاسلكي تعمل على حماية الشبكات اللاسلكية من التهديدات، وتمكين المسؤولين لكشف ومنع هجمات الشبكة المختلفة.

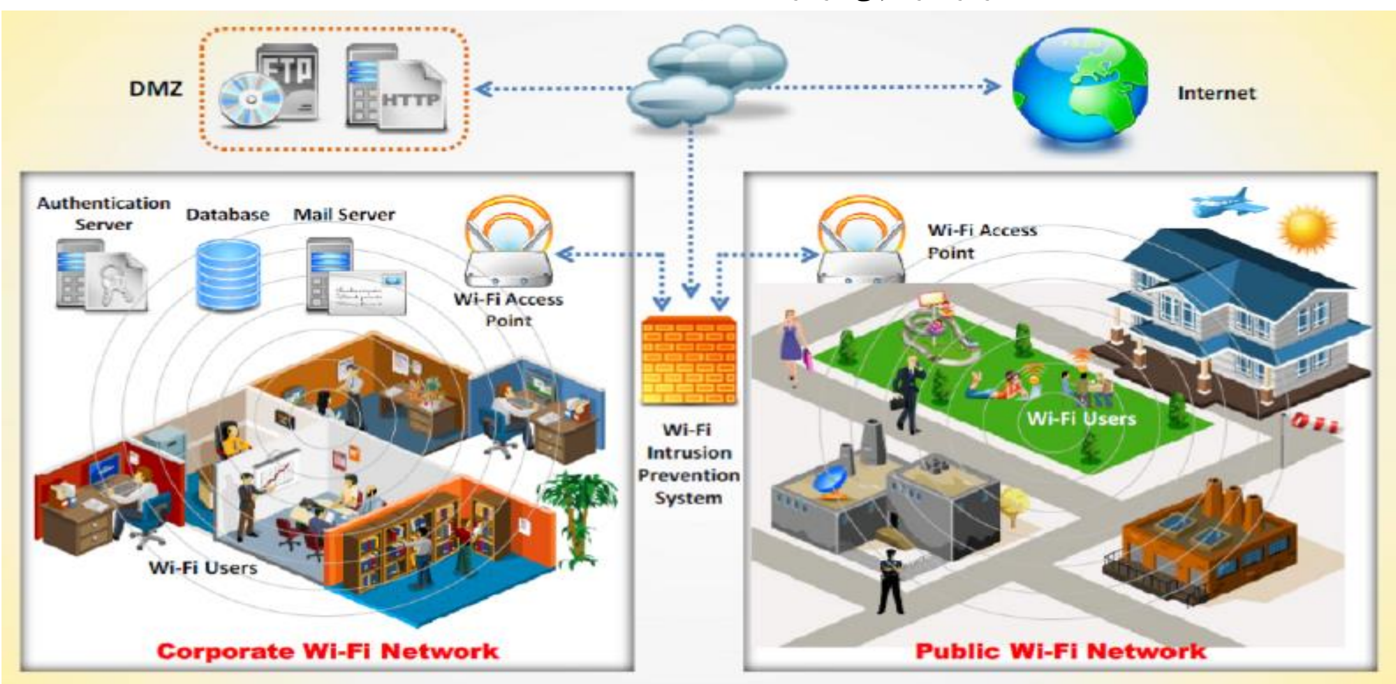


WIRELESS IPS DEPLOYMENT

WIPS تتكون من عدد من المكونات التي تعمل معا لتوفير عملية رصد أمنيه موحده.

وظائف المكونات الموجودة في Cisco's Wireless IPS Deployment:

- **Access points in monitor mode**: توفر قناة ثابته للفحص مع الكشف عن الهجوم وقدرات التقاط الحزم.
- **Mobility services engine (running wireless IPS service)**: النقطة المركزية لتجميع الإنذار من كافة وحدات تحكم ومن الوحدات اللاسلكية المتكاملة لرصد وضع نقاط الوصول. يتم تخزين معلومات الإنذار وملفات **forensic** على النظام لأغراض الأرشيف.
- **Local mode access point(s)**: يوفر الخدمة اللاسلكية للعملاء بالإضافة إلى فحص الموقع.
- **Wireless LAN Controller(s)**: يوجه الهجوم على المعلومات من **wireless IPS Monitor Mode Access point's** إلى **MSE** ويوزع معلمات التكوين الى نقاط الوصول.
- **Wireless control system**: يوفر الى المسئول الوسيلة لتكوين الخدمة اللاسلكية المتكاملة في **MSE**، ودفع اعدادات **IPS** اللاسلكية الى وحدة التحكم، وتعيين نقاط الوصول الى **wireless IPS monitor mode**. كما أنها تستخدم لعرض إنذارات **IPS** اللاسلكية، **forensics**، والوصول إلى موسوعة التهديد.



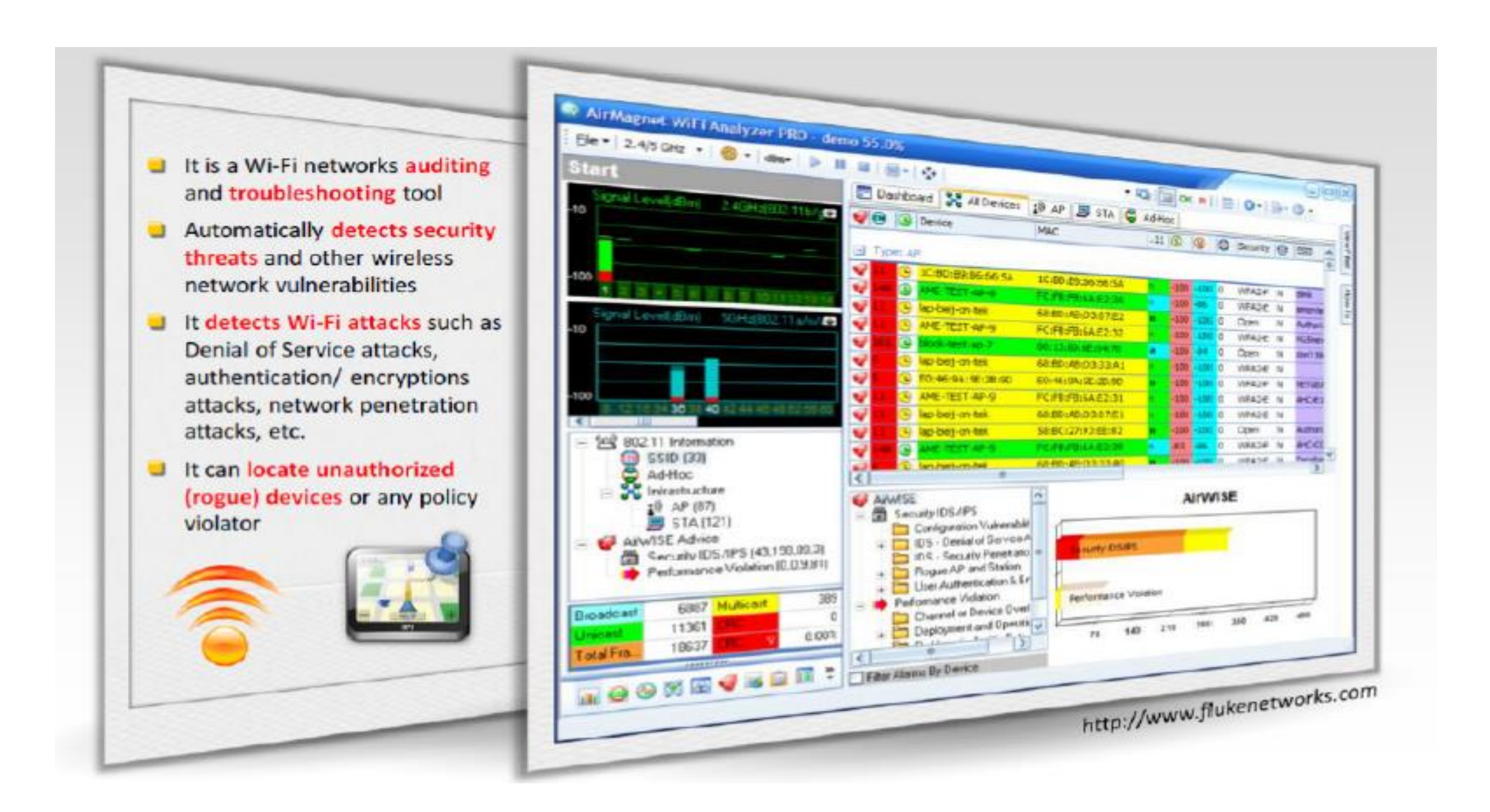
WI-FI SECURITY AUDITING TOOL: AIRMAGNET WIFI

المصدر: http://www.flukenetworks.com

AirMagnet WiFi Analyzer هي أداة موحدة من اجل **mobile auditing** واستكشاف الأخطاء وإصلاحها في شبكات الواي فاي. وهو يساعد موظفي تكنولوجيا المعلومات على حل قضايا المستخدم أثناء الكشف التلقائي عن التهديدات الأمنية ومواطن الضعف في شبكة الاتصال اللاسلكية. الحل يتيح لمديري الشبكة اختبار وتشخيص العشرات من القضايا في الأداء اللاسلكي بما في ذلك قضايا الإنتاجية ومشاكل الاتصال وتعارضات الأجهزة ومشاكل الإشارات المتعددة القنوات. وهو يشمل محرك لإنشاء تقرير كامل، والذي فيه يتم تعيين معلومات شبكة الاتصال التي تم جمعها إلى الاحتياجات اللازمة للامتثال للأنظمة السياسة والصناعة.

AirMagnet WiFi Analyzer متوفر في الإصدارات **Express** و **Pro**. **Express** يوفر البنات الأساسية للاسلكي وإصلاحها ومراجعة الحسابات مع القدرة على رؤية الأجهزة، تحديد المشاكل المشتركة تلقائياً، وفعليا تحديد موقع أجهزة محددة. الإصدار **Pro** يشمل إلى حد كبير كل الإمكانات الموجودة في الإصدار **Express** ويضيف الكثير لتوفير أداة لاسلكيه لحل أي نوع من تحديدات الأداء أو الأمن.

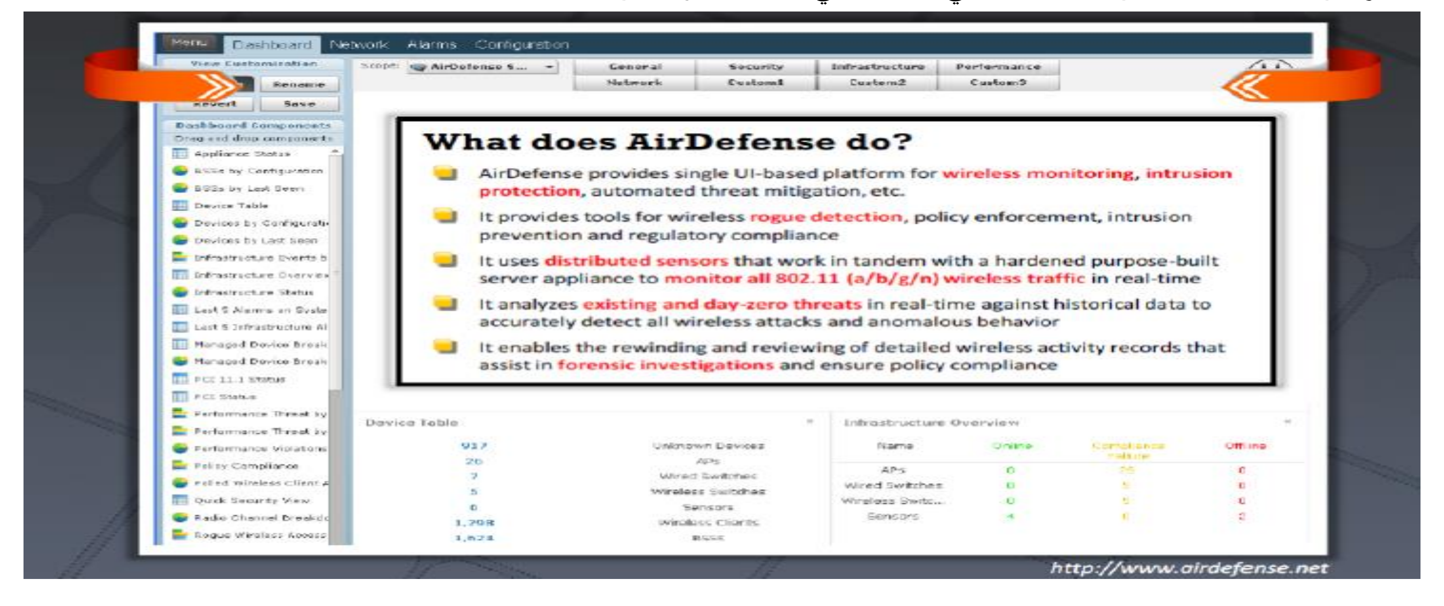
AirMagnet WiFi Analyzer يمكنه الكشف عن الهجمات على الشبكة اللاسلكية مثل هجمات دوس، هجمات المصادقة/التشفير، هجمات اختراق الشبكة، إلخ. ويمكنه بسهولة تحديد موقع الأجهزة الغير مصرح بها (المارقة) أو المنتهكة السياسة.



WI-FI SECURITY AUDITING TOOL: AIRDEFENSE

المصدر: https://www.airdefense.net

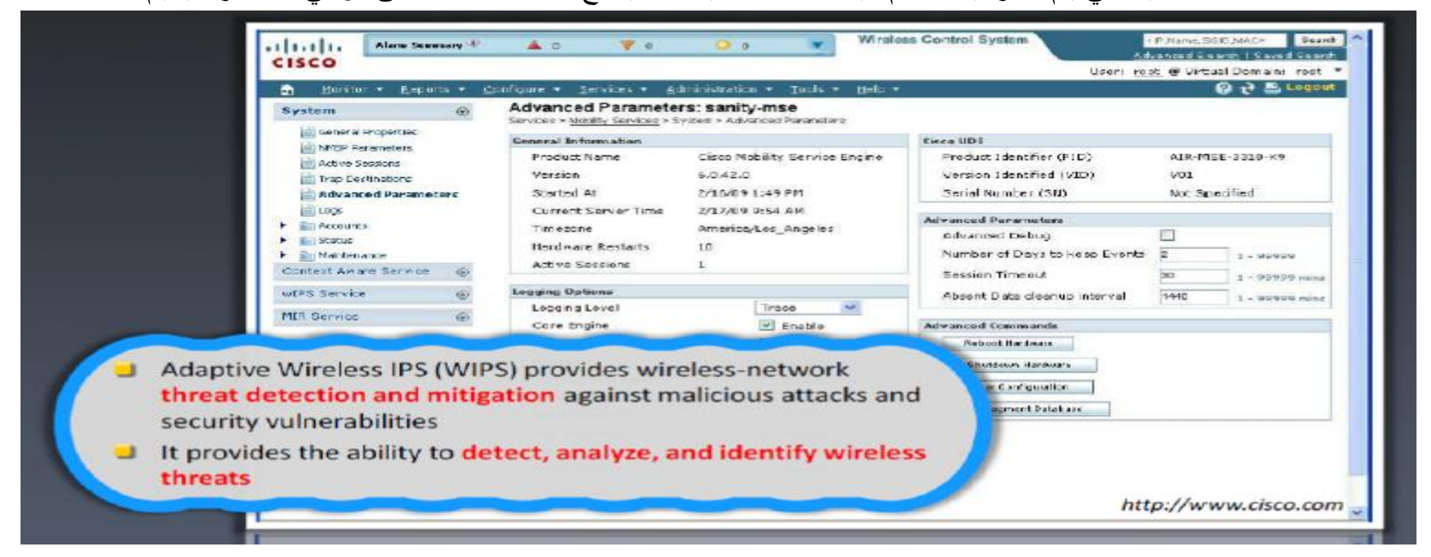
AirDefense يوفر منصة واحدة لرصد الشبكة اللاسلكية، الحماية من الاختراق، والتخفيف من حدة التهديد، إلخ. فإنه يوفر أدوات لكشف الشبكات اللاسلكية المارقة وإنفاذ السياسات ومنع التسلل والامتثال للوائح التنظيمية. ويستخدم أجهزة استشعار موزعه والتي تعمل في ترادف مع جهاز خادم بنيا لهذا الغرض لرصد جميع حركة مرور الشبكات اللاسلكية **802.11 (a/b/g/n)** في الوقت الحقيقي. ويحلل التهديدات القائمة وتهديدات اليوم صفر في الوقت الحقيقي ضد البيانات التاريخية للكشف بدقة عن جميع الهجمات اللاسلكية والسلوك الشاذ. وهي تمكن استعراض سجلات مفصلة عن النشاط اللاسلكي للمساعدة في التحقيقات، وضمان الامتثال للسياسة.



WI-FI SECURITY AUDITING TOOL: ADAPTIVE WIRELESS IPS

المصدر: http://www.cisco.com

Adaptive Wireless IPS (WIPS) يوفر الكشف عن تهديد شبكة محددة والتخفيف من حدتها ضد الهجمات الخبيثة والثغرات الأمنية ومصادر لتعطل الأداء. يوفر القدرة على اكتشاف وتحليل وتحديد التهديدات اللاسلكية. كما أنها يوفر قدرات الوقاية من التهديدات وذلك من اجل تصلب الشبكة اللاسلكية التي يتم اختراقها بمعظم الهجمات اللاسلكية، مما يسمح للعملاء الحفاظ على الوعي المستمر ببيئتهم **RF**.



WI-FI INTRUSION PREVENTION SYSTEM

أنظمة منع اختراق الوأي فأي يعمل على غلق التهديدات اللاسلكية من خلال الفحص تلقائياً، والكشف، وتصنيف الوصول اللاسلكي الغير مصرح به جميعا ونقاط الوصول المارقة على شبكة الاتصال، وبالتالي منع المستخدم المجاور أو المتسللين المهرة الوصول الغير مصرح به إلى موارد الشبكة اللاسلكية. عدد قليل من أنظمة منع اختراق الوأي فأي كما يلي:

Enterasys® Intrusion Prevention System available at http://www.enterasys.com
RFProtect Wireless Intrusion Protection available at http://www.arubanetworks.com
HP TippingPoint IPS available at http://h17007.www1.hp.com
AirTight WIPS available at http://www.airtightnetworks.com
Network Box IDP available at http://www.network-box.co.uk
AirMobile Server available at http://www.airmobile.se
WLS Manager available at http://www.airpatrolcorp.com
Wireless Policy Manager (WPM) available at http://www.airpatrolcorp.com
ZENworks Endpoint Security Management available at http://www.novell.com

WI-FI PREDICTIVE PLANNING TOOLS

أدوات **Wi-Fi predictive planning**، تخطط بنجاح، تنشر وترصد وتستكشف الأخطاء وتصلحاها وتقدم تقرير عن الشبكات اللاسلكية الداخلية والخارجية من الموقع المركزي. أدوات **Wi-Fi predictive planning**، كما يلي:

AirMagnet Planner available at http://www.flukenetworks.com
Cisco Prime Infrastructure available at http://www.cisco.com
AirTight Planner available at http://www.airtightnetworks.com
LANPlanner available at http://www.motorola.com

RingMaster available at http://www.juniper.net
Connect EZ Predictive RF CAD Design available at http://www.connect802.com
Ekahau Site Survey (ESS) available at http://www.ekahau.com
ZonePlanner available at http://www.ruckuswireless.com
Wi-Fi Planning Tool available at http://www.aerohive.com
TamoGraph Site Survey available at http://www.tamos.com

WI-FI VULNERABILITY SCANNING TOOLS

أدوات فحص نقاط الضعف في الشبكات اللاسلكية هي التي تحدد مواطن الضعف في الشبكات اللاسلكية وتأمينها قبل قيام المهاجمين باستخدامها لمهاجمة الشبكات اللاسلكية واختراقها. فيما يلي عدد قليل من هذه الادوات:

Zenmap available at http://nmap.org
Nessus available at http://www.tenable.com
OSWA available at http://securitystartshere.org
Network Security Toolkit available at http://networksecuritytoolkit.org
Nexpose Community Edition available at http://www.rapid7.com
WiFish Finder available at http://www.airtightnetworks.com
Penetrator Vulnerability Scanning Appliance available at http://www.secpoint.com
SILICA available at http://www.immunityinc.com
Wireless Network Vulnerability Assessment available at http://www.secnap.com

الحمد لله تعالى، وبحول الله تعالى نكون قد انتهينا من الوحدة الخامسة عشر من CEHv8. ونلقاكم مع الوحدة التالية:

د. محمد صبحي طيبه